

التجارة الإلكترونية

د. أحمد سلام عبد العاطي
جامعة الإسكندرية - كلية التجارة

مؤسسة طيبة للنشر والتوزيع

التجـارة الإلكترونية

د. أحمد سلام عبد العاطي

جامعة الإسكندرية – كلية التجارة

الناشر

مؤسسة طيبة للنشر والتوزيع

7 شارع علام حسين – ميدان الظاهر – القاهرة

ت -0227876470 /0227867198

فاكس/ 0227876471

محمول/ 01112155522 – 01091848808

الطبعة الاولى 2021

فهرسة أثناء النشر من دار الكتب والوثائق القومية المصرية

عبد العاطي ؛ أحمد سلام .

التجارة الإلكترونية / أحمد سلام عبد العاطي .– القاهرة : مؤسسة طيبة للنشر والتوزيع 2021

238 ص ؛ 24 سم .

تدمك : 1 -537 -431 -977 -978

1 – التجارة الإلكترونية

أ -العنوان

380,02853

رقم الإيداع : 7989/ 2021

بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

ٱقْرَأْ بِٱسْمِ رَبِّكَ ٱلَّذِى خَلَقَ ﴿١﴾ خَلَقَ ٱلْإِنسَٰنَ مِنْ عَلَقٍ ﴿٢﴾ ٱقْرَأْ وَرَبُّكَ ٱلْأَكْرَمُ ﴿٣﴾ ٱلَّذِى عَلَّمَ بِٱلْقَلَمِ ﴿٤﴾ عَلَّمَ ٱلْإِنسَٰنَ مَا لَمْ يَعْلَمْ

صدق الله العظيم

مقدمة

بدأ مصطلح التجارة الإلكترونية في الظهور بعد عام 1994 ، حيث أن هذا المصطلح ارتبط وبشكل كامل مع اختراع شبكة الانترنيت Internet والتي غزت العالم بشكل منقطع النظير ، فشبكة الانترنيت تعد من أهم اختراعات هذا العصر والتي استطاعت ربط دول العالم بشكل لم يكن من الممكن تخيله سابقا. ولا بد من التعرف على شبكة الانترنيت أولا قبل التعرف على التجارة الإلكترونية وخصوصا لخلط البعض بين مفهوم شبكة الانترنيت العالمية Internet و الشبكة العنكبوتية العالمية (WWW) وهو اختصار World Wide Web .

الفصل الأول

تأثير التجارة الإلكترونية على نظم المعلومات المحاسبية

الفصل الأول

تأثير التجارة الإلكترونية على نظم المعلومات المحاسبية

تمثل التجارة الإلكترونية أحد مجالات التطور في إستخدام تقنيات المعلومات الحديثة من حيث إمكانية الأستفادة من هذه التقنيات في تسهيل القيام بالعمليات التجارية إستناداً إلى البيانات المتعلقة بها والتي يمكن تجميعها وخزنها ومعالجتها وتداولها بين العديد من الجهات ذات العلاقة بالنواحي التجارية أو الأقتصادية .

ونظراً للتطورات السريعة والمذهلة التي صاحبت إستخدام التجارة الألكترونية من قبل العديد من الشركات العالمية في بلدان مختلفة ، فقد تطلب الأمر من الكثير من الشركات الأخرى أن تعد الدراسات اللازمة لكيفية دخول عالم التجارة الألكترونية لكي تستطيع مواكبة هذه التطورات والسير في طريقها لكي تتمكن من تحقيق أهدافها أسوة بالعديد من الشركات التي تحقق فوائد في ظل التجارة الألكترونية .

وبما أن نظم المعلومات المحاسبية تمثل نظماً رسمية ورئيسية في أي شركة من الشركات ، كما أنها تمثل نظماً مفتوحة تؤثر في البيئة التي تعمل في نطاقها وتتأثر بها ، فقد أصبح من الضروري الأخذ بنظر الأعتبار التأثيرات التي يمكن أن تنعكس على نظم المعلومات المحاسبية وكيفية تصميمها وتحديد طبيعة عملها في تلك الشركات التي تعمل في ظل التجارة الألكترونية ، ومن هنا تأتي مشكلة البحث .

أما أهمية البحث فتأتي من خلال محاولة التعرض إلى موضوع حديث يتعلق بإحدى إستخدامات تقنيات المعلومات وهو التجارة الألكترونية ومناقشة مدى إمكانية تأثيره على نظم المعلومات المحاسبية .

عليه فإن البحث يهدف إلى تحقيق الآتي :-

1. توضيح طبيعة التجارة الألكترونية وعلاقاتها بعمل نظم المعلومات المحاسبية في الشركات التي تعمل في ظلها .

2. تحديد أهم تأثيرات التجارة الألكترونية على مكونات نظم المعلومات المحاسبية

3. تحديد أهم تأثيرات التجارة الألكترونية على مقومات نظم المعلومات المحاسبية.

4.تحديد أهم تأثيرات التجارة الألكترونية على طبيعة نظم المعلومات المحاسبية .

ولغرض تحقيق أهداف البحث يتم الأعتماد على الفرضيتين الآتيتين :

1.إن إزدياد التعاملات الأقتصادية في ظل التجارة الألكترونية سوف يفرض على نظم المعلومات المحاسبية أن تطور من أساليبها ومكوناتها في سبيل الوفاء باحتياجات الشركات التي تعمل في ظل التجارة الألكترونية .

2. إن التأثيرات على نظم المعلومات المحاسبية في ظل التجارة الألكترونية سوف تتعلق بالتأثير على مكونات نظم المعلومات المحاسبية (المادية والبشرية) وكذلك على مقوماتها وأيضاً على طبيعة عملية تصميمها في الشركات التي تعمل في ظل التجارة الألكترونية .

أما منهج البحث الذي يتم الأعتماد عليه فهو المنهج الوصفي وذلك من خلال الأستعانة بالمصادر العلمية ذات العلاقة بموضوعات : نظم المعلومات المحاسبية التجارة الألكترونية، نظم المعلومات الأدارية ، تقنيات المعلومات والأتصالات .

وقد تم تقسيم خطة البحث إلى أربعة مباحث أساسية تناول المبحث الأول منها طبيعة التجارة الألكترونية وعلاقاتها بعمل نظم المعلومات المحاسبية في الشركات التي تعمل في ظلها ، بينما تناول المبحث الثاني مناقشة تأثير التجارة الألكترونية على المكونات المادية والبشرية لنظم المعلومات المحاسبية ، وتناول المبحث الثالث تحديد تأثير التجارة الألكترونية على المقومات الرئيسية لنظم المعلومات المحاسبية التي تشمل كلاً من : المجموعة المستندية ، المجموعة الدفترية ، دليل الحسابات مجموعة التقارير والقوائم المالية ، أما المبحث الرابع فتناول تأثير التجارة الألكترونية على طبيعة نظم المعلومات المحاسبية من حيث إمكانية تصميمها وعلاقاتها بنظم المعلومات الأخرى في ظل التجارة الألكترونية .

المبحث الأول . طبيعة التجارة الألكترونية وعلاقتها بعمل نظم المعلومات المحاسبية

أولاً . طبيعة التجارة الألكترونية .

تمثل التجارة الألكترونية Electronic Commerce أحد مجالات إستخدام تقنيات المعلومات والأتصالات الحديثة والتي ظهرت مفاهيمها وتطورت سبل دراستها والبحث فيها وتقييمها خلال السنوات القليلة الماضية .

إن إنتشار إستخدام الوسائل الألكترونية الحديثة في العديد من مجالات الحياة قد ساهم في البحث عن إمكانية إستخدامها في مجال عالم الأعمال بصورة عامة ومجال الأعمال التجارية بصورة خاصة ، وهو ما يشير إلى ظهور مصطلح " التجارة الألكترونية " الذي يركز على ممارسة عمليات الترويج والأعلان والبيع والشراء للسلع والخدمات بإستخدام الوسائل الألكترونية المتعددة .

ونظراً للمزايا العديدة التي يمكن أن يحققها الأنترنت في تحقيق أهداف الأعمال التجارية فقد تم إستخدامه بصورة أكبر وأكثر من غيره من المجالات التي تعتمد على الحاسبات الإلكترونية وبالتالي فإنه غالباً ما يرتبط مفهوم التجارة الألكترونية بالأنترنت وبالتالي فهو يمثل جزءاً مهماً وأساسياً ضمن مفهوم التجارة الألكترونية .

ولتوضيح مفهوم التجارة الألكترونية يمكن أن نتطرق إلى مجموعة من التعاريف التي وضعها الكتاب والباحثون أهمها :

1. حسب ما جاء في تعريف منظمة التجارة العالمية هي " توزيع السلع والخدمات وتسويقها بالوسائل الألكترونية " .[1]

2. هي عمليات الأعلان والتعريف للبضائع والخدمات ثم تنفيذ عمليات عقد الصفقات وإبرام العقود ثم الشراء والبيع لتلك البضائع والخدمات ثم سداد القيمة الشرائية عبر شبكات الأتصال المختلفة سواء الأنترنت أو غيرها من الشبكات التي تربط بين المشتري والبائع.[2]

3. مفهوم جديد يشرح عملية بيع أو شراء المنتجات والخدمات والمعلومات من خلال شبكات كمبيوترية ومن ضمنها الأنترنت ن وهناك عدة وجهات نظر من أجل تعريف هذا المصطلح : فعالم الأتصالات يعرف التجارة الألكترونية بأنها وسيلة من أجل إيصال المعلومات أو الخدمات أو المنتجات عبر خطوط الهاتف أو عبر الشبكات الكمبيوترية أو عبر أي وسيلة تقنية . ومن وجهة نظر الأعمال التجارية فهي عملية تطبيق التقنية من أجل جعل المعاملات التجارية تجري بصورة تلقائية وسريعة . في أن الخدمات تعرف التجارة الألكترونية بأنها أداة من أجل تلبية رغبات الشركات والمستهلكين والمدراء في خفض كلفة الخدمة والرفع من كفاءتها والعمل على تسريع إيصال الخدمة . وأخيراً فإن عالم الأنترنت يعرفها بالتجارة التي تفتح المجال من أجل بيع وشراء المنتجات والخدمات والمعلومات عبر الأنترنت .[3]

4. مجموعة متكاملة من عمليات إنتاج وتوزيع وتسويق وبيع المنتجات بوسائل إلكترونية ، كما أنها تعتبر وسيلة من وسائل إيصال المعلومات أو الخدمات أو المنتجات عبر خطوط الهاتف أو عبر الشبكات الكمبيوترية ، كما أنها أداة من أدوات تلبية رغبات الشركات والمستهلكين ورجال العمال في خفض تكاليف الخدمات والرفع من كفاءتها والعمل على تسريع إيصال الخدمة إلى مستحقيها .[4]

. [1]www. Bluenilctadcpoint. Com / arabisitc / c-comers / arabicindcx-copy (23) .

[2] د. رأفت عبد العزيز غنيم ، دور جامعة الدول العربية في تنمية وتيسير التجارة الألكترونية بين الدول العربية ، جامعة الدول العربية - إدارة قطاعات الخدمات الأساسية ، نوفمبر ، 2002 . ص 4 .

. [3]www. Rccf . com / modulcs . php? Namc= ncws$ filc = articlc& sid= 21 .

[4] . 1 www. Hosinganimc. Com / smartshop / ccommcrcc. html (إستخدام التجارة الألكترونية للترويج عن الأستثمار في السودان) .

5. أداء العمليات التجارية بين الشركات بعضها البعض ، الشركات والحكومات من خلال إستخدام تكنولوجيا المعلومات وشبكة الأتصالات في أداء تلك العمليات وتهدف إلى رفع الكفاءة في الأداء وتحقيق الفاعلية في التعامل ، إنها تتعدى الحدود الزمنية التي تقيد حركة التعاملات التجارية ، وتتيح إستجابة سريعة لطلبات السوق من خلال التفاعل مع العملاء ، وتعمل على تبسيط الإجراءات ووضوح إجراءات العمل.[1]

ومن خلال ما تقدم يمكن القول أن التجارة الألكترونية هي نظام متكامل يتعلق بممارسة العمليات التجارية (من بيع وشراء) وما تتطلبه من إعلان وتوصيل للمعلومات وتسديد واستلام للمبالغ المترتبة عنها ، وذلك باستخدام الوسائل الألكترونية المعتمدة على الشبكات بين الشركات أو العملاء التي يحدث بينها هذا النوع من المعاملات ، ونظراً للمزايا العديدة التي تتمتع بها عملية إستخدام الأنترنت فإنه يمثل الأساس الأهم في ممارسة التجارة الألكترونية ، حيث يمثل الأنترنت أحد الوسائل المهمة والمتقدمة ضمن تقنيات المعلومات الحديثة .

وللتجارة الألكترونية مجموعة من الأنماط التي تدور حولها بحيث يمكن النظر إلى التجارة الألكترونية على أنها مفهوم متعدد الأبعاد يمكن تطبيقه واستخدامه في أكثر من نمط وشكل وكما يلي :-[2]

1. مؤسسة أعمال. مؤسسة أعمال .

يتم هذا النمط بين مؤسسات الأعمال بعضها البعض من خلال شبكات الاتصالات وتكنولوجيا المعلومات ، وذلك لتقديم طلبات الشراء للموردين والعارضين و تسليم الفواتير و إتمام عمليات الدفع ، وهذا النمط من التجارة الإلكترونية موجود من سنوات عديدة خاصة في تبادل البيانات إلكترونياً من خلال الشبكات الخاصة .

---

[1] . . www. Shamela. Net / vb / archive / index. Php / (بحث بعنوان البنوك الألكترونية) .

[2] . لمزيد من الأطلاع أنظر :-

- د. رأفت عبد العزيز غنيم ، مصدر سابق ، ص ص 4-6 .
- د. رأفت رضوان ، عالم التجارة الألكترونية ، المنظمة العربية للتنمية الأدارية ، القاهرة ، 1999 . ص ص 29- 33 .
- European Commission , Accelerating Electronic Commerce in Europe : Technology Development & Business Pilot Projects, European Commission , 1998.

2.مؤسسة أعمال . مستهلك .

هذا النمط من التجارة الألكترونية يمثل البيع بالتجزئة في التبادل التجاري العادي ، وقد توسع بشكل كبير مع ظهور شبكة الأنترنت ، فهناك الآن ما يسمى بـ " المراكز التجارية للتسوق shopping malls " تقدم خدماتها من خلال عرض السلع والخدمات لصالح المؤسسات وتقوم بتنفيذ الصفقات التجارية من حيث عمليات الشراء والبيع من خلال شبكات الأنترنت ويتم الدفع بطرق مختلفة أكثرها شيوعاً بطاقات الأئتمان أو الشيكات الإلكترونية أو نقداً عند التسليم .

3.مؤسسة أعمال . إدارة حكومية .

هذا النمط يغطي كل المعاملات بين الشركات والهيئات الحكومية . حيث يمكن الأعلان عن المشتريات الحكومية من خلال شبكة الأنترنت ويمكن للشركات أن تتبادل الردود معها إلكترونياً (كما هو الحال في الولايات المتحدة) . وحالياً يعتبر هذا النمط في مرحلة وليدة ، لكنه سوف يتوسع بسرعة كبيرة إذا قامت الحكومات باستخدام عملياتها بأسلوب التجارة الألكترونية .

4.مستهلك . إدارة حكومية .

هذا النمط لم يبزغ بعد ، لكنه ربما ينتشر مع إنتشار التعامل الألكتروني ونمو كل من نمط الشركة إلى المستهلك والشركة إلى الهيئة الحكومية .

ثانياً . علاقة التجارة الألكترونية بعمل نظم المعلومات المحاسبية .

يمثل نظام المعلومات المحاسبية (AIS) " أحد النظم الفرعية في الوحدة الاقتصادية يتكون من عدة نظم فرعية تعمل مع بعضها البعض بصورة مترابطة ومتناسقة ومتبادلة ، بهدف توفير المعلومات التاريخية والحالية والمستقبلية ، المالية وغير المالية لجميع الجهات التي يهمها أمر الوحدة الاقتصادية ، وبما يخدم تحقيق أهدافها ".[1]

[1] . زياد هاشم يحيى و د. قاسم محسن الحبيطي ، نظام المعلومات المحاسبية ، وحدة الحدباء للطباعة والنشر ، كلية الحدباء الجامعة ، الموصل ، العراق ، 2003 . ص 41 .

وبما ان توجه العديد من الوحدات الأقتصادية نحو إستخدام التجارة الألكترونية أخذ يزداد شيئاً فشيئاً من حيث أنه يمثل أحد التغيرات والتطورات التي يجب أن تحقق الوحدات الأقتصادية الفائدة التي يمكن أن تساعدها نحو تحقيق أهدافها ، وبما أن نظام المعلومات المحاسبية هو نظام مفتوح يؤثر ويتأثر بالبيئة التي يعمل في نطاقها كما أنه يمثل النظام الرسمي للمعلومات في أي وحدة إقتصادية وبالتالي يقع على عاتقه أن يوفر المعلومات المختلفة للعديد من الجهات التي لها علاقة بالوحدة الأقتصادية المعنية . إضافة إلى إمكانية تحقيق أهدافه وأهداف الوحدة الأقتصادية التي يعمل فيها . ، فإن الأمر يتطلب من نظم المعلومات المحاسبية في الوحدات الأقتصادية . التي تعمل في ظل التجارة الألكترونية . أن تأخذ بنظر الأعتبار كل التغيرات والتطورات التي تحدث في المجالات المتعددة المحيطة ببيئتها وخاصة ما يتعلق بالتطورات المستجدة في مجال إستخدام تقنيات المعلومات والأتصالات الحديثة والتي تمثل التجارة الألكترونية إحداها .

عليه يمكن القول أن علاقة التجارة الألكترونية بعمل نظم المعلومات المحاسبية سوف يتطلب من نظم المعلومات المحاسبية أن تأخذ بالمستجدات التي سوف تفرزها متطلبات العمل في ظل التجارة الألكترونية خاصة ما يتعلق بضرورة إستخدام الوسائل الألكترونية الحديثة في العمل المحاسبي وكذلك إعادة تصميم النظام بما يتلاءم مع عملية التشغيل الألكتروني للبيانات وما يتبعه من تأثيرات أخرى سواء على مكونات أو مقومات النظام والتي سوف نتناولها في المباحث اللاحقة .

المبحث الثاني - تأثير التجارة الألكترونية على مكونات نظم المعلومات المحاسبية .

تتعلق مكونات نظام المعلومات المحاسبية - بصورة عامة - بمجموعة من الأجزاء البشرية والمادية ،[1] وفي ظل التشغيل اليدوي للبيانات فإن النظام سوف يعتمد بصورة رئيسية على الكادر البشري إضافة إلى مجموعة من الوسائل الآلية أو شبه الآلية البسيطة التي تساعد على القيام بالعمل المحاسبية ، ولكن عند قيام الوحدة الأقتصادية بالعمل في ظل التجارة الألكترونية فإن الأمر يتطلب ضرورة إستخدام الوسائل الألكترونية والتي يشكل الأنترنت أحد أهم هذه الوسائل وبما يعني أن العديد من البيانات يجب أن تعتمد على التشغيل الألكتروني باستخدام الحاسبات وملحقاتها الأمر الذي يتطلب من نظام المعلومات المحاسبية أن يعتمد على التشغيل الألكتروني للبيانات ، وهو ما يدعو إلى الحاجة لتطوير مكوناته بحيث تشمل كل الوسائل التي يتطلبها العمل في ظل التجارة الألكترونية .

وبذلك فإن مكونات نظام المعلومات المحاسبية في ظل التجارة الألكترونية سوف تشمل كلاً من : مجموعة الأفراد المؤهلين ، أجهزة الحاسوب ، البرمجيات ، قاعدة البيانات ، الأجراءات ، تقنيات الأتصالات ، وكما يلي :-

أولاً - مجموعة الأفراد المؤهلين .

يشكل الأفراد أحد المكونات الأساسية لنظام المعلومات المحاسبية ، وتزداد أهمية وجود الأفراد ضمن مكونات نظام المعلومات المحاسبية في ظل العمل لأغراض التجارة الألكترونية من حيث ضرورة وجود الأفراد المؤهلين - علمياً وعملياً - ومدى قدرتهم على أداء العمل المحاسبي في ظل إستخدام التقنيات الحديثة وتعدد الجهات التي تتكون لها علاقات مع الوحدة الأقتصادية التي يتم العمل فيها وكذلك زيادة البيانات والمعلومات التي يتطلب تجميعها وتشغيلها وتوصيلها إلى الجهات المعنية .

ونظراً لأهمية عنصر الافراد ضمن إدارة عمل نظم المعلومات المحاسبية فإن نظام المعلومات المحاسبية يمكن أن يشمل مجموعة من الأفراد تضم كلاً من :-

[1] - المصدر السابق ، ص 17 .

1.المحاسبين بكافة درجاتهم الوظيفية (مديري حسابات ، محاسبين ، معاوني محاسبين ، كتاب حسابات) ، والذين يقع على عاتقهم القيام بكافة الاعمال المحاسبية من تسجيل وتبويب وتلخيص وعرض للبيانات المحاسبية والمساعدة على برمجتها على الحاسبة الإلكترونية والتأكد من دقة ذلك بصورة دورية مستمرة.

2.محللو ومصممو نظام المعلومات المحاسبية ، الذين يقع على عاتقهم القيام بعمليات تحليل وتصميم نظام المعلومات المحاسبية أو أي من نظمه الفرعية عندما يستدعي الأمر ذلك .

3.المحللون الماليون ، الذين يقع على عاتقهم تحليل القوائم المالية الأساسية والأضافية التي ينتجها نظام المعلومات المحاسبية في الوحدة الاقتصادية ، أو تحليل أي بيانات أخرى لها علاقة بعمل نظام المعلومات المحاسبية .

4. المبرمجون ، الذين يقع على عاتقهم القيام بعمليات البرمجة التي يستلزمها عمل الحاسبات الإلكترونية .

5.أي افراد اخرين ضمن جهات لها علاقة بعمل نظام المعلومات المحاسبية في سبيل تبادل المعرفة ومحاولة الاستفادة منها بصورة متبادلة بين نظام المعلومات المحاسبية وأي نظم معلومات أخرى يمكن أن تتواجد ضمن الوحدة الاقتصادية أو خارجها .

ثانياً . أجهزة الحاسوب.

وهي تمثل الوسيلة الأساسية في عمل نظام المعلومات المحاسبية عند العمل في ظل التجارة الألكترونية نظراً لأنه لا يمكن أداء العمل بدونها سواء من حيث تشغيل البيانات ومعالجتها بالسرعة والدقة المطلوبتين أو من حيث إمكانية إجراء الأتصالات مع الجهات التي يتم التعامل معها وتوصيل البيانات والمعلومات اللازمه لها .

كما إن إستخدام أجهزة الحاسوب في عمل نظم المعلومات المحاسبية يمكن أن يؤدي إلى الأستفادة من الخصائص الاتية :- [1]

[1] . إخلاص هزاع الجبدلي ،إستخدام الوسائل الآلية في نظام المعلومات المحاسبية ـ وسائل مقترحة في مصرف الرافدين / نينوى / 112 ، رسالة ماجستير في المحاسبة ، كلية الأدارة والأقتصاد ـ جامعة الموصل ، 2003 . ص ص 5-6 .

. -السماح بتشغيل البيانات المحاسبية بطريقة مرنة قادرة على إنتاج معلومات متعددة من حيث الكم والنوعية في ظل جميع البدائل الممكنة بوقت قصير جداً وعلى درجة عالية من الدقة بمعنى ان استخدام الوسائل الآلية يُسهم في تحقيق وتوافر الخصائص النوعية الرئيسة في المعلومات المحاسبية (الملائمة والثقة).

2. -إن إستخدام الحاسوب يؤدي إلى تحقيق الرقابة الداخلية والذاتية على تنفيذ العمليات بحيث يمكن تلافي الأخطاء في مراحل التشغيل المختلفة أولاً بأول ، حيث يتضمن الحاسوب وسائط للضبط والرقابة والتحقق من النتائج .

3. ان استخدام الحاسوب يساعد على إنجاز الأعمال الحسابية والإدارية بسرعة وبالتالي يؤدي إلى تخفيض التكاليف، وخاصة في الحالات التي تزداد فيها تكلفة العمالة اليدوية عن تكلفة التشغيل الآلي ولهذا يرى الكثير من مصممي النظم المحاسبية ان أي آلة مكتبية يجب ان تعطي عائد يغطي تكلفتها في سنة أو سنين ويتمثل هذا العائد في وفورات رواتب الموظفين.

4. ان استخدام الحاسوب يوفر إمكانية إنتاج مستندات متعددة بعملية آلية واحدة وهذه المستندات اما ان تكون نسخا متعددة من مستند محاسبي واحد أو مستندات وسجلات محاسبية تستخدم لاستيفائها نفس البيانات.

5. يساعد استخدام الحاسوب في تطبيق أساليب المعرفة الأخرى مثل أساليب بحوث العمليات وتزاوجها مما يساعد بدوره على إنشاء نظام متكامل للمعلومات المحاسبية والإدارية وفتح آفاق جديدة للأبحاث والدراسات العلمية .

6. يتيح التشغيل الآلي للبيانات توفير كمية هائلة من المعلومات المحاسبية وغيرها التي يمكن استخدامها في أغراض مختلفة كالتخطيط والرقابة واتخاذ القرارات.

7. يتم تطبيق مبدأ كتابة البيانات مرة واحدة حيث يتم إدخال البيانات في المرة الأولى ويتم تغيير البيانات الموجودة في جميع الملفات المتعلقة بها مباشرة في نفس الوقت ويتم استخراج التقارير تلقائيا.

8. القدرة التخزينية وسرعة استرجاع المعلومات للحاسوب أدى إلى مركزه المعلومات في جهاز معين مما يترتب عليه أخطار مختلفة من عمليات الاختراق وان حماية المعلومات من هذه الأخطار هو السبيل الوحيد والعملي للحفاظ عليها ومثل هذه المسئولية مناطة برؤساء الوحدات الاقتصادية التي تتعامل بالمعلومات وتحفظها في مختلف وسائط الحفظ .

9. ان استخدام الحاسوب يهيئ الفرصة للوحدات الاقتصادية لبناء هياكلها التنظيمية بشكل اكثر مرونة فغالبا الوحدات التي لا تعتمد على الحاسوب يحدث لديها تأخير في معالجة وتوصيل المعلومات خلال الهيكل التنظيمي وفي مثل هذه الحالة فان استخدام الحاسوب من شأنه ان يوفر المرونة في اختيار الهيكل التنظيمي الملائم بما يساعد في تقلص هذا التأخير.

ثالثاً . البرمجيات .

وهي تتضمن مجموعة من التعليمات التشغيلية الموجهة للحاسوب يقوم باتباعها لتنفيذ الأهداف المطلوبة من النظام ، ويمكن التفرقة بين نوعين أساسيين من البرامجيات وهي برامج النظام وبرامج التطبيقات .[1]

ومن أمثلة البرامجيات : [2]

آ. البرامج التي ينفذها الحاسبة (البرامج المعيارية) .

ب. البرامج الجاهزة (التطبيقات الجاهزة) .

جـ. البرامج المساعدة .

د. البرامج المترجمة .

هـ. أنظمة تشغيل الأقراص .

وتمثل برامج التشغيل (البرامج التطبيقية) كافة البرامج التي يمكن الاستعانة بها في عمل نظام المعلومات المحاسبية في الوحدة الاقتصادية والتي يتم من خلالها تنفيذ مجموعة من الأوامر والتعليمات التي يتم تغذية الحاسب بها لكي تتمكن

[1] . د. محمد عبد الفتاح محمد و طارق عبد العال حماد ، التطبيقات المحاسبية باستخدام الحاسب ، الدار الجامعية ، الأسكندرية ، 2000 ،ص 30 .

[2] . زياد هاشم يحيى و د. قاسم محسن الحبيطي ، مصدر سابق ، ص 174 .

من استقبال البيانات المختلفة وتوجيهها حسب العمليات المحاسبية اللازمة بهدف استخراج المعلومات المطلوبة .

وتشمل برامج التشغيل التي يمكن استخدامها في مجالات عمل نظام المعلومات الحاسبية بدرجة أساسية كافة البرامج التطبيقية المحاسبية التي يمكن الاستعانة بها دون الحاجة إلى مبرمج لبرمجة العمليات المحاسبية واستخراج نتائجها .

رابعاً - قاعدة البيانات .[1]

تمثل قاعدة البيانات المحاسبية مجموعة من الملفات المرتبطة مع بعضها البعض بصورة منطقية ومخزونة بطريقة منظمة تسهل وصول البرامج التطبيقية إليها بهدف معالجة البيانات .

ويمثل وجود قاعدة البيانات ضمن مكونات نظام المعلومات المحاسبية أمراً هاماً حيث أن ذلك يساعد على تحقيق الفوائد الآتية:

1. تحتوي قاعدة البيانات المحاسبية على كافة البيانات التي لها علاقة بكافة أنشطة الوحدة الاقتصادية التي تقوم بها الإدارات والأقسام المختلفة فيها ، مما يؤدي إلى سهولة الوصول إلى أي بيانات ينبغي معالجتها بصورة مباشرة وسريعة.

2. إن وجود البيانات ضمن قاعدة البيانات بصورة موحدة (مركزية) سوف يؤدي إلى تقليل تكرار عملية حفظ البيانات (في حالة تعدد وجودها ضمن ملفات مستقلة) الأمر الذي يساهم أيضاً في تخفيض تكاليف حفظ البيانات نظراً لعدم الحاجة إلى تكرار الملفات ذات البيانات المتشابهة .

3. المساهمة في تحقيق حالة التكامل بين النظم الفرعية للمعلومات في الوحدة الاقتصادية من خلال إمكانية إمداد وتبادل البيانات فيما بينها من خلال مصدر موحد متمثل بقاعدة البيانات الأمر الذي يساهم في تقليل الوقت والجهد المبذول في ذلك.

[1] . المصدر السابق ، ص ص 180-181 .

4.سهولة تجميع البيانات ومعالجتها من قبل المستخدمين (وخاصة من داخل الوحدة الاقتصادية) الأمر الذي يساهم في تقديم المعلومات (المخرجات) بسرعة وبالتالي زيادة كفاءة القرارات التي يمكن أن تتخذ بناءاً عليها.

وهناك عدة طرق تستخدم لتنظيم قاعدة البيانات تعتبر جميعها في غاية الأهمية بالنسبة لنظم المعلومات المحاسبية حيث أنها تؤثر على طريقة تنظيم السجلات المحاسبية على ملفات الحاسبة الإلكترونية ، ومن ثمّ على كيفية استخدام بيانات هذه الملفات في إعداد التقارير المالية . وحيث أن قاعدة البيانات ليست إلا ملفات الحاسبة الإلكترونية ، التي تقلل من تكرار البيانات إلى أدنى حد ممكن ،والتي يمكن الوصول إليها بواسطة شخص محدد أو أكثر ، فانه يمكن اتباع أي تنظيم للملفات التي تستخدم في إنشاء قاعدة البيانات .

خامساً- الإجراءات .

ويقصد بها مجموعة السياسات والأساليب التي ينبغي اتباعها عند استخدام وتشغيل والتعامل مع نظام المعلومات فعلى سبيل المثال تتمثل الإجراءات التي يجب اتباعها لتشغيل برنامج الرواتب في تحديد موعد تشغيل البرنامج (نهاية الشهر منتصف الشهر، ...الخ) ومن له سلطة تشغيل البرنامج ومن له حق الاطلاع على مخرجات هذا النظام من كشوفات الرواتب وإشعارات الاضافة وغيره .[1]

سادساً- تقنيات الأتصالات .[2]

يقصد بها : كافة الأنشطة والوسائل المتعلقة بالنقل الإلكتروني للمعلومات والبيانات من موقع لآخر باستخدام الأجهزة والبرامج والوسائط او القنوات التي تربط بين الحاسبات وبعضها أو بين الحاسبات وبعض الوحدات الآلية الأخرى .

وتتخذ عملية الربط شكل شبكة يطلق عليها " شبكة الحاسبات " التي تعرف بانها " مجموعة حاسبات مرتبطة مع بعضها البعض أو مع بعض الوحدات الالية الاخرى

[1] . طارق طه ، إدارة البنوك ونظم المعلومات المصرفية ، الحرمين للكومبيوتر ، الأسكندرية ، 2000 ,ص 509 .

[2] . المصدر السابق ، ص ص 509-511 .

(كالشاشات والطابعات وغيرها) بمواقع متقاربة او متباعدة مكانيا من خلال وسائط او قنوات اتصال بحيث يمكن لاي وحدة داخل الشبكة ان تتبادل البيانات وتستخدم الموارد المادية وغير المادية لباقي اعضاء الشبكة مع احتفاظها بقدراتها التشغيلية الخاصة بها " وشبكات الاتصال تكون على نوعين:

1. الشبكات ذات النطاق المحدود (المحلية):وهي الشبكات التي تغطي مواقع متقاربة مكانياً كالتي تربط بين الحاسبات داخل الشركة.

2. الشبكات ذات النطاق المتسع: وهي الشبكات التي تغطي مواقع متباعدة مكانيا كالتي تربط بين الحاسبات لفروع المصرف المختلفة داخل الدولة او تربط بين حاسوب الشركة والحاسوب بمركزها الرئيسي في دولة اخرى .

ولاستخدام تلك الشبكات بصورة اكثر فاعلية تعتمد الشركات على ما يعرف بالبرامج الجماعية التي تتيح نمط تفاعلي سريع بين مستخدمي الشبكة من خلال عرض المستندات التي يتم التعامل معها على اكثر من شاشة في وقت واحد وهو ما يتيح لموظفي المصرف التعرف على المتغيرات التي تطرأ على كل مستند لحظة بلحظة .

وتتم خطوط الاتصال ذات النطاق المتسع عادة عبر خطوط لنقل الاتصالات وتختلف تركيبة الرموز المستعملة في ارسال البيانات عبر هذه الخطوط عن خصائص رموز البيانات الموجودة في الحاسوب ويعني هذا وجوب ترجمة اسلوب الترميز من الحاسوب الى خطوط نقل الاتصالات ومن ثم اعادة ترجمته عند موقع الحاسوب التالي ويتم ذلك بواسطة اجهزة خاصة من اهمها اجهزة المحولات واجهزة التحويل المتعدد وتتم عمليات الاتصال من خلال قنوات عديدة اهمها الخطوط الارضية وانظمة الارسال اللاسلكية والاقمار الصناعية الخاصة بالاتصالات .[1]

[1] . اتحاد المصارف العربية ، التدقيق والأمان والرقابة في ظل إستخدام الحاسبات الألكترونية ، مطابع امير قيو ، بيروت ، 1989 . ص

المبحث الثالث. تأثير التجارة الألكترونيـــة على مقومات نظم المعلومات المحاسبية

يعتمد نظام المعلومات المحاسبية . في أي وحدة إقتصادية . على مجموعة من المقومات الرئيسة التي يتم العمل المحاسبي بواسطتها وهي تشمل كلاً من : المجموعة المستندية ، المجموعة الدفترية ، دليل الحسابات ، مجموعة التقارير والقوائم المالية ، وتشكل هذه المقومات مرتكزات أساسية لا يمكن الأستغناء عن أي منها مهما كانت طريقة تشغيل البيانات المتبعة . يدوية أم إلكترونية . ، ونظراً لأعتماد نظام المعلومات المحاسبية على التشغيل الألكتروني للبيانات في حالة العمل في ظل التجارة الألكترونية فإن هناك تأثيراً مباشراً على مقومات النظام يمكن توضيحها كما يلي:[1]

أولاً. الأثر على المجموعة المستندية .

ان الأعتماد على التشغيل الألكتروني للبيانات يتطلب ضرورة تعديل شكل وطبيعة هذه المستندات أو استخدام مجموعة مستندية جديدة تشتمل على البيانات الموجودة في المستندات الأصلية بصورة تتماشى مع البرنامج المحاسبي الإلكتروني الذي يطبق في الوحدة الاقتصادية وكذلك نظام الترميز المتبع للوصول إلى البيانات التي تم حفظها بواسطة الشريط المغنط أو الاقراص المغنطة.

ثانياً . الأثر على المجموعة الدفترية .

في ظل الطريقة المحاسبية التي تتبعها الوحدات الاقتصادية تتعدد الدفاتر المحاسبية ولكن عند الأعتماد على التشغيل الألكتروني للبيانات تعد ذاكرة الحاسوب والأشرطة المغنطة والأقراص المغنطة بمثابة الدفاتر المحاسبية. وقد ترتب على تعدد برامج المحاسبة في الأسواق اعداد دفاتر إلكترونية متعددة ومتنوعة تناسب اعمال واحجام الوحدات الاقتصادية المختلفة مما ادى إلى سهولة التعامل

---

[1] . لمزيد من الأطلاع يمكن الرجوع إلى :-
- د. أحمد حلمي جمعة ، التدقيق الحديث للحسابات ، دار صفاء للنشر والتوزيع ، عمان ، الأردن ، 1999. ص ص 164-165.
- إنعام محسن حسن زويلف ، أثر إستخدام الحاسوب في الأداء المحاسبي - دراسة تطبيقية في عينة من المنشآت الصناعية العراقية ، أطروحة دكتوراه في المحاسبة ، كلية الأدارة والأقتصاد - الجامعة المستنصرية ، 1996 . ص 13 .
- إخلاص هزاع كريم العبدلي ، مصدر سابق ، ص ص 19-22 .

مع هذه الدفاتر وسرعة فائقة جدا في العمليات المختلفة عند التسجيل أو التعديل أو الالغاء أو الاستفسار.

ثالثاً. الأثر على دليل الحسابات .

ان الأعتماد على التشغيل الألكتروني للبيانات قد ساعد على تطوير طريقة الإعداد للدليل المحاسبي فضلاً عن المحافظة على سرية البيانات أو الحسابات المسجلة . اجمالية كانت ام فرعية . وكذلك دقة التصنيف للحسابات.

رابعاً. الأثر على مجموعة التقارير والقوائم المالية .

أدى الأعتماد على التشغيل الألكتروني للبيانات إلى دقة وسرعة الحصول على التقارير (اليومية – الاسبوعية – الشهرية – الفصلية – السنوية)، فضلاً عن إمكانية عرضها على شاشة العرض المرئي وبالتالي سرعة تغير المعلومات التي تضمها التقارير قبل طباعتها أو تخزينها.

إضافة لما تقدم ، فإن الوحدة الاقتصادية تهدف من التشغيل الإلكتروني للبيانات إلى توفير مزيد من السرعة والدقة فضلاً عن تزويد الإدارة بالتقارير اللازمة ولا يتحقق ذلك الا في ظل نظام جيد تتوافر فيه عناصر الرقابة الكافية ويجب ان يشمل نظام الرقابة الداخلية النظام بكامله بمعنى الجزء الآلي والجزء الذي بقي يدوياً كما يجب ان تبنى قواعد الرقابة الداخلية في المدخلات والمخرجات فضلاً عن مرحلة التشغيل التي تميزت بانخفاض العنصر البشري وهنا يلاحظ ان استخدام الحاسوب قد اثر في كل من الرقابة الإدارية والرقابة الإجرائية .

فبالنسبة للرقابة الادارية فإنها تشير إلى الفصل في الهيكل التنظيمي بين الوظائف المتعارضة ويمثل هذا الفصل احد اساليب الرقابة الوقائية السليمة التي تقضي بعدم السماح لموظف واحد بالجمع بين عدد من الوظائف المترابطة حتى يمكن تلافي مخاطر السرقة والاختلاس والتلاعب بموجودات الوحدة الاقتصادية وسجلاتها. ولتحقيق اهداف الرقابة الادارية يجب اولا تحديد الموقع المناسب لادارة الحاسوب في الهيكل التنظيمي للوحدة الاقتصادية ككل ويختلف هذا الموقع من وحدة

إلى أخرى حسب حجم الوحدة وطبيعة نشاطها والسياسات المتبعة من قبلها وبعد دراسة الموقع الذي يمكن ان تتخذه إدارة الحاسوب في الهيكل التنظيمي للوحدة الاقتصادية يجب دراسة التنظيم الداخلي السليم لهذه الادارة حيث يمثل التنظيم الداخلي السليم عامل هام يساعد على زيادة الثقة في نظام الرقابة الداخلية ولتحقيق مزيد من الثقة لابد من توضيح الحدود الفاصلة بين الوظائف الأساسية لهذه الإدارات فضلاً عن تحديد مواصفات هذه الوظائف والسلطات والمسؤوليات الملقاة على عاتقهم.

أما الرقابة الإجرائية فتهدف إلى تأكيد صحة وشمولية معالجة البيانات المحاسبية وان لا يتداول تلك البيانات المعالجة إلا من يصرح لهم وتقسم أساليب الرقابة الإجرائية في ظل المعالجة الإلكترونية للبيانات إلى ثلاث مجموعات وهي : أساليب الرقابة على المدخلات وأساليب الرقابة على معالجة البيانات وأساليب الرقابة على المخرجات، وكما يلي :

1. أساليب الرقابة على المدخلات : وتهدف إلى توفير درجة تأكد معقولة من صحة اعتماد البيانات (التي يستلمها قسم معالجة البيانات) بواسطة موظف مختص ومن سلامة تحويلها بصورة تمكن الحاسوب من التعرف عليها ومن عدم فقدانها أو الإضافة إليها أو الحذف منها أو طبع صورة منها أو عمل أي تعديلات غير مشروعة في البيانات المرسلة حتى وان كان ذلك من خلال خطوط الاتصال المباشر وتشمل أساليب الرقابة على المدخلات تلك الأساليب التي تتعلق برفض تصحيح أو إعادة إدخال البيانات السابق إدخالها.

2. أساليب الرقابة على معالجة البيانات : وتهدف إلى توفير درجة تأكد معقولة من تنفيذ عمليات معالجة البيانات إلكترونياً طبقا للتطبيقات المحددة.

3. أساليب الرقابة على المخرجات : تهدف إلى تأكيد دقة مخرجات عمليات معالجة البيانات وتداول هذه المخرجات بواسطة الاشخاص المصرح لهم فقط.

كما إن الأعتماد على التشغيل الألكتروني للبيانات المحاسبية أدى إلى افتقاد أغلب مستندات التدقيق وكذلك ظهور أخطار محيطة بعملية التشغيل وحماية البيانات ويمكن القول على نحو عام انه قد ترتب على ذلك حدوث تغيير في طبيعة مسار

المراجعة وبالتالي تغيير في إجراءات التدقيق بصيغة عامة. وقد أوضحت الدراسات ان من أهم العوامل التي شجعت على حدوث سرقات ومخاطر التزوير في الوحدات الاقتصادية التي تستخدم الحاسوب في تشغيل البيانات المحاسبية وهو عدم فهم مدققي الحسابات طبيعة عمل الحاسوب بالدرجة الأولى فالمعالجة الإلكترونية للبيانات لا تغير من أهداف التدقيق وإنما تؤثر في طريقة تشغيل وتخزين البيانات المحاسبية. ومما يتبع ذلك من وجوب تطويع إجراءات التدقيق لملائمة بيئة التشغيل الجديدة. وقد حدد دليل التدقيق الدولي رقم (401) دور المدقق في هذه الحالة بأنه: يجب على مدقق الحسابات في ظل ظروف المعالجة الإلكترونية للبيانات ان يتفهم المكونات المادية للحاسوب وكذلك البرامجيات ونظم المعالجة الإلكترونية بالقدر الذي يمكنه من تخطيط عملية التدقيق وتفهم آثار استخدام الحاسوب في تقييم ضوابط الرقابة الداخلية ، وتطبيق إجراءات التدقيق وخاصة أساليب التدقيق الفنية المساعدة كما يجب على المدقق ان يكون على قدر كاف من الإلمام بتشغيل البيانات المحاسبية بالشكل اللازم لتنفيذ إجراءات التدقيق اعتماداً على منهج التدقيق المطبق.

كذلك أوضحت الدراسات أنه من أهم عوامل حدوث السرقات هو عدم اتفاق إجراءات التدقيق مع طبيعة وبيئة المعالجة الإلكترونية للبيانات مما دعا إلى ضرورة أحداث تغيير في تكنولوجيا التدقيق خاصة في مجالات استخدام الحاسوب والأساليب الإحصائية والرياضيات وأساليب التحليل الكمي وذلك يمثل أهم الاتجاهات المعاصرة في التدقيق فلكي يكون المدقق قادراً على تقويم نظام الرقابة الداخلية لا بد أن يكون متفهماً للجوانب الفنية في تشغيل البيانات المحاسبية والمشكلات المرتبطة بها.

1. لكي تحقق نظم المعلومات المحاسبية وتساهم في تحقيق أهداف الشركات التي تعمل فيها، لابد أن تأخذ بنظرالأعتبار كل التغيرات والتطورات التي تحدث في المجالات المتعددة المحيطة ببيئتها وخاصة ما يتعلق بالتطورات المستجدة في مجال إستخدام تقنيات المعلومات والأتصالات الحديثة والتي تمثل التجارة الألكترونية إحداها .

2. إن إنضمام العديد من الشركات للعمل في ظل التجارة الألكترونية يتطلب من نظـم المعلومات المحاسبية إعادة وتقييم مكوناتها وأساليبها المستخدمة في تجميع البيانـات وتخزينها ومعالجتها ومن ثم توصيلها إلى الجهات التي يمكن أن تعتمد عليها في إتخاذ القرارات المتعددة.

3.أن عمل نظم المعلومات المحاسبية في الشركات التي تعمل في ظل التجارة الألكترونية يتطلب الأهتمام بالكادر البشري (المتمثل بالأفراد القائمين على عمل نظم المعلومات المحاسبية) وتطوير مهاراته المعرفية في مجالات إستخدام أساليب تقنيات المعلومات لكي يكون بمقدوره التعامل معها وتحقيق الفائدة من إستخدامها في مجال عمل نظم المعلومات المحاسبية .

4.إن العمل في ظل التجارة الألكترونية سوف يؤثر على المقومات الأساسية لنظم المعلومات المحاسبية والمتمثلة بكل من : المجموعة المستندية ، المجموعة الدفترية ، دليل الحسابات، مجموعة التقارير والقوائم المالية ، الأمر الذي يتطلب ضرورة الأخذ بنظر الأعتبار هذه التأثيرات وآنعكاساتها على عملية تصميم نظم المعلومات المحاسبية .

5.إن طبيعة نظم المعلومات المحاسبية في ظل التجارة الألكترونية سوف تؤدي إلى ضرورة إعتماد الوسائل الألكترونية في عملية تصميمها ، إضافة إلى ضرورة الأخذ بنظر الأعتبار علاقات التنسيق والترابط مع نظم المعلومات الأخرى التي تعمل في الشركة المعنية وخاصة نظم المعلومات الأدارية ، وصولاً إلي تحقيق نظام متكامل للمعلومات المحاسبية والأدارية يعمل من خلال وجود قاعدة بيانات مركزية يمكن من خلالها تحقيق أكبر فائدة في عمل النظام وكذلك سرعة البيانات وتوصيل المعلومات الناتجة عنها إضافة إلى المساهمة في تحقيق الجدوى الأقتصادية من عملية تصميم وعمل النظام .

1. ضرورة مواصلة البحث العلمي في تحديد ودراسة أهم تأثيرات إستخدام الأساليب الأخرى لتقنيات المعلومات والأتصالات الحديثة على نظم المعلومات المحاسبية .

2. إمكانية تعزيز الدراسة الحالية بدراسة ميدانية في عدد من الشركات التي تعمل في ظل التجارة الألكترونية . وخاصة في العراق . للوقوف على مدى الأخذ بنظر الأعتبار هذه التأثيرات على نظم المعلومات المحاسبية من الناحية التطبيقية .

3. ضرورة إحتواء المواد الدراسية وخاصة مادة نظم المعلومات المحاسبية على مفردات خاصة باستخدام أساليب تقنيات المعلومات والأتصالات بصورة عامة والتجارة الألكترونية بصورة خاصة ، بهدف تهيئة الكادر المحاسبي الذي يتم تخريجه من الكليات والمعاهد العلمية على كيفية فهم طبيعة عمل هذه الأساليب وكذلك كيفية إستخدامها في عمل نظم المعلومات المحاسبية .

الفصل الثاني

التسويق والتجارة الالكترونية التشفيرية

الفصل الثاني

التسويق والتجارة الالكترونية التشفيرية

لقد فاقت الإحصائيات والتوقعات جميع التصورات ، ويأتي ذلك نتيجة للتطور الهائل في الإنترنت التي ستقوم بإعادة صياغة الاقتصاد العالمي من جديد ولا تقتصر التجارة الإلكترونية على المبادرات التي تتم بين التاجر والمستهلك ، وهو المجال الذي تستحوذ فيه الكتب والاسطوانات المبرمجة وأجهزة وبرامج الكمبيوتر وخدمات السفر وحجز التذاكر والخدمات المالية ، على النصيب الأكبر من هذا القطاع ولكن التقديرات تشير إلى ان المجال الأكثر سرعة في نمو التجارة الإلكترونية والأكثر توقعاً لتحقيق نجاح عاجل وكبير هو العمليات التي تتم بين القطاعات التجارية فيما بينها فالعمليات الإلكترونية التي تكون بين مؤسسة تجارية وأخرى عادة ما تكون استمراراً للعلاقات التجارية الموجودة المدعومة بدرجة عالية من الثقة والمعززة بواسطة عقود ثابتة ، وكما ان تطوير أي علاقة ثابتة طويلة الأجل إلى استخدام الوسائل الإلكترونية ليس تحويلا إلى تجارة الإلكترونية فحسب ، وإنما هو في الواقع وسيلة لإحداث وتحقيق مكاسب كبيرة للطرفين من خلال التطبيق لهذه الوسائل تعد العمليات التجارية التي تتم بين نشاطين تجاريين هو المجال الذي يمكن للتجارة الإلكترونية ان تقدم من خلاله مكاسب كبيرة بشكل واضح وذلك عن طريق توحيد إجراءات التوريد ميكنة عملية الشراء وفي التقديم المتميز والأفضل للخدمات المساندة للعملية التجارية ، وكذلك توفير الوقت من خلال الاعتماد على المراسلات الآلية ، والإلغاء التدريجي للتعامل الورقي مما سيؤدي بالتالي إلى تقليل التكاليف المرتبطة بإعداد أوامر الشراء والبيع والتحويل إلى أسلوب الشراء الإلكتروني ولا ننسي فتح مصادر جديدة للتوريد يعطي أصحاب المصانع فرصة للحصول على مواد أولية أقل سعرا وبالتالي تنخفض السعر النهائي للمستهلك .

أهداف البحث :

من خلال ممارسة التجارة الإلكترونية نجد من الصعب تحديد أهداف التجارة الإلكترونية بشكل دقيق وواضح لما تواجهه نشاطات الأعمال على اختلاف أنواعها من مشاكل كثيرة في تحديد هدف معين فالمتغيرات الداخلية والخارجية بما فيها من اضطراب في الأسواق يصعب عمليا الجزم بتحقيق الهدف تماما . كون بعض المشروعات قد تخسر بشكل أو بآخر معتمدة على أمل تعويض خسائرها في المستقبل عندما تكون قد رسخت نفسها وأسست لنفسها صورة في أذهان المستهلك . وبشكل عام يمكن القول أن هناك بعض الأهداف التي تسعي المشروعات لبلوغها أو تعمل باتجاه تحقيقها من خلال ارتباطها بالسياسات التجارية أو الصناعية على مستوي السوق العالمي كما أن الإنترنت يلعب دوراً هاماً في التجارة الإلكترونية .

أهمية البحث : -

1. التعريف بالتجارة الإلكترونية وكيفية التعامل بها من اجل ان نواكب العصر الحديث حيث ان السنوات المقبلة ستشهد نمواً كبيراً في حجم هذه التجارة نتيجة عوامل خارجية وداخلية معاً .
2. توفير الجهد والوقت في العمليات التجارية من خلال التجارة الإلكترونية لأنها قد تكون الوسيلة الأفضل على الإطلاق والحل المناسب .
3. العمل على مساعدة المهتمين في رسم الخطط للإدارات داخل المنظمات.
4. العمل على تحقيق النمو والازدهار على كافة المستويات.
5. المساهمة بفتح أسواق جديدة والعمل على إيصال السلع للمستهلك بالمكان والزمان.
6. العمل على تسهيل المعاملات التجارية من خلال تحسين المستوى التقني لتحقيق رغبات المستهلكين والشركات.

فرضية البحث :

كلما زاد انتشار التجارة الإلكترونية أثر ذلك على القطاع التجاري .

لمحة تاريخية عن نشأة التجارة الإلكترونية:

يتضح من أن مفهوم التسويق في حقبة من الزمن لما كان يختصر على عملية بيع وشراء بسيطة تتم بين المنتج والبائع والمشتري في أسواق محددة ولم يكن هناك نشاطاً تسويياً بمعنى الكلمة واستمر الحال على ذلك إلى أن بدأت التجارة بين البلدان عبر البر والبحر واستمر الحال إلى أن قامت الثورة الصناعية منذ ظهور الآلة البخارية وتطور الإنتاج من حيث الكم والنوع وبقي السوق في البداية سوق منتجين على اعتبار العطش من السلع والمنتجات كان موجوداً وظل التسويق من حيث الاهتمام به متواضعاً وكان مفهوم آنذاك بالمفهوم البيعي للتسويق الذي يقتصر على الإعلام وتعريف المستهلك بالسلعة وبالتالي تتم عملية البيع والشراء، ومع مرور الزمن والتطور التكنولوجي والعلمي في حياتنا ظهر الإنتاج الكبير وتحسنت نوعيته وظهرت المنافسة بين المنظمات في جميع بلدان العالم وخاصة بعد تطور الاتصالات والنقل السريع في هذه الظروف أصبح السوق في معظم بلدان العالم سوق مستهلك حيث أصبح عرض المنتجات أكبر من الطلب عليها فالمستهلك الذي يريد شراء سيارة أصبح أمامه عشرات البدائل والشركات المنتجة جميعها تحاول كسب أكبر حصة أو نسبة من السوق.

ما هي التجارة الإلكترونية؟

لم يتبلور حتى الآن مفهوم نهائي للتعاملات التجارية التي تتم عبر الإنترنت والتي تدعى حالياً بالتجارة الإلكترونية ، ويقال حالياً إن العالم يشهد كل يوم تطورات جديدة تضاف إلى شكل ومضمون المفهوم الحالي للتجارة الإلكترونية، وقد يؤدي تبني أحد اللاعبين الكبار في سوق تقنيات المعلومات لأحد المفاهيم الجدية مستقبلاً إلى إبطال استخدام هذا الاسم وإحلال اسم جديد محله، وحتى هذا المفهوم الحالي للتجارة الإلكترونية ما زال غامضاً بعض الشيء على الرغم من أنه مضى

على استخدام تقنيات هذه التجارة عدة سنوات وعلى الرغم من الانتشار الهائل الذي تشهده الأعمال التجارية عبر الإنترنت ما زالت تظهر يومياً مفاهيم موازنة جديدة مثل التسوق الإلكتروني، ومقدمي خدمات التطبيقات، والأعمال المصرفية عبر الإنترنت وغيرها من المفاهيم ، ويوجد ارتباط وثيق بين هذه المسميات إذ تدخل جميعاً تحت مظلة التجارة الإلكترونية بحيث يصعب إعطاء تعريف أحدهما من دون الإشارة إلى الآخر ([1]) ، والتجارة الإلكترونية بصفة أساسية "هي إدارة أي نشاط تجاري من خلال الشبكات" وقد يعني هذا بصفة عامة "شبكة من أجهزة الكمبيوتر المتصلة ببعضها البعض، ويكون هذا الاتصال بين تلك الأجهزة من خلال شبكة تسمى "الإنترنت" ([2]) .

لفظة التجارة الإلكترونية:

أما بالنسبة للفظة التجارة الإلكترونية فقد تم اشتقاقها باللغة الإنجليزية من (Electronic commerce) ويقصد بها عملية حوسبة التجارة، أي استخدام تكنولوجيا الحاسوب في العمليات التجارية، أما (I-commerce) فهي مشتقة من (Internet commerce) أي التجارة عبر الإنترنت، وتعبر التجارة عبر الإنترنت جزء من التجارة الإلكترونية ، ولكن اليوم اعتاد العالم على استخدام اللفظيين بطريقة تبادلية بسبب أن معظم نشاطات التجارة الإلكترونية يتم عبر الإنترنت ([3]) .

تعريف التجارة الإلكترونية:

يعتبر أكثر التعريفات شيوعاً للتجارة الإلكترونية هو تعريف منظمة التجارة العالمية لها وهي: تنفيذ بعض أو كل العمليات التجارية في السلع والخدمات عبر شبكة الإنترنت والشبكات التجارية العالمية الأخرى ، أي باستخدام تكنولوجيا المعلومات والاتصالات ، وهي وسيلة سريعة وسهلة لإبرام الصفقات التجارية الإلكترونية، سواء كانت التجارة في السلع والخدمات أم في المعلومات وبرامج الكمبيوتر ([4]).

تعاريف أخرى للتجارة الإلكترونية:

- بأنها نظام يتيح عبر الإنترنت حركات بيع وشراء السلع والخدمات والمعلومات.
- هي نوع من عمليات البيع والشراء ما بين المستهلكين والمنتجين أو بين الشركات بعضهم وبعض باستخدام تكنولوجيا المعلومات والاتصالات.
- أنها أداء العملية التجارية بين الشركاء التجاريين باستخدام تكنولوجيا معلومات متطورة بغرض رفع كفاءة وفاعلية الأداء.
- هي استخدام تكنولوجيا المعلومات لإيجاد الروابط الفعالة بين الشركاء في التجارة.
- هي منهج حديث في الأعمال موجه إلى السلع والخدمات وسرعة الأداء ويشمل استخدام شبكة الاتصال في البحث والاسترجاع للمعلومات لدعم اتخاذ قرار الأفراد والمنظمات.
- هي شكل من أشكال التبادل التجاري باستخدام شبكة الاتصالات بين الشركات بعضها وبعض الشركات وعملائها أو بين الشركات والإدارة العامة.
- هي مزيج من التكنولوجيا والخدمات للإسراع بأداء التبادل التجاري وإيجاد آلية لتبادل المعلومات داخل الشركة وبين الشركة والشركات الأخرى والشركة والعملاء (بيع وشراء).

أقسام التجارة الإلكترونية:

من تعريف التجارة الإلكترونية بأنها ممارسة جميع الأعمال التجارية عبر الإنترنت يمكن الاستنتاج أنه لكل عملية تجارية تتم بالطرق التقليدية هناك مقابل لها في التجارة الإلكترونية ومن هنا يمكن تقسيم نشاطات التجارة الإلكترونية بشكلها الحالي إلى أقسام منها ما هو رئيسي ومنها ما هو ثانوي:

أولاً: الأقسام الرئيسية وهي قسمين:

- تجارة الأعمال مع المستهلكين: ويطلق عليها أيضاً اسم التسوق الإلكتروني وتتوجه نحو المستهلك حيث تكون العلاقة بين المستهلك كفرد والبائع علاقة مباشرة يتم من خلالها تسويق السلعة ويقوم المستهلك بالبحث عنها ومقارنة المواصفات والأسعار مع المواقع الأخرى.

وتنتهي هذه العملية عادة بتسجيل طلب الشراء والقيام بدفع مقدماً عبر الشبكة كامل المبلغ أو جزء منه من خلال بطاقة الائتمان في الغالب وتقوم الجهة البائعة بتوصيل البضاعة عبر وسطاء الشحن لعنوان المستهلك، وتشير اتجاهات التجارة الإلكترونية في هذا النوع تبعاً لدراسات تحليلية إلى أن (4٪) من العرب تعاملوا بهذا النوع مقابل (24٪) في الولايات المتحدة تعاملوا مع إجمالي المتعاملين مع التجارة الإلكترونية.

- تجارة الأعمال مع الأعمال: يتم من خلال هذا النوع من التجارة الإلكترونية مكننة الأعمال بين الشركات التي تتعامل مع بعضها البعض وهنا تختلف أساليب التعامل عن تجارة المستهلك حيث أن التعامل بين الشركات يتجاوز عملية البيع والشراء المباشر، وتتم هذه التعاملات من خلال الاتصال بالشركة أو المؤسسة من خلال احتياطات أمان تتمثل في كلمات سر للدخول وعناوين ويب خاصة وهذا النوع من التجارة ناجح جداً، بدأ في الآونة الأخيرة يطغى على ساحة التجارة الإلكترونية حيث تفيد الإحصاءات أن التجارة الموجهة بين التجار تفوق التجارة الموجهة نحو الأفراد بعشرة أضعاف على الأقل، هذه الإحصاءات قامت بها (Abderdeen Group) كما يتوقع لهذه الفئة أن تشهد نمواً مركباً بمعدل 41٪ في السنوات القادمة نتيجة لإحصاءات (Yankee Group) ، ومن المتوقع أن يبلغ إجمالي راس مال التجارة الموجهة بين التجار عام 2006 ما مقداره 12.41 مليار دولار، وهذه إحصاءات (Gartener Group).

وأحد الأسباب في نجاح هذا القسم من التجارة الإلكترونية هو كون هذا النوع لا يتميز بنفس الدرجة من المجازفة التي تواجهها الشركات مع الأفراد ([5]) .

ثانيا: الأقسام الثانوية (غير الرئيسية) وهي ثلاثة أقسام:

- تجارة الأعمال مع الحكومة: وهذا القسم من التجارة يمثل العلاقة بين الإدارات الحكومية والشركات فيمكن للحكومة أن تعمم قراراتها إلى الشركات عن طريق نشرها على صفحات الإنترنت وتستطيع الشركات الرد على ذلك عن طريق نفس الطريقة، كذلك تستطيع تلك الشركات دفع الضرائب وتعبئة النماذج وهكذا ....

- تجارة المستهلك مع الحكومة: وهو ما يتعلق بالإدارات الحكومية والأفراد فيمكن للحكومة أيضاً في هذا القسم من أن تعمم قراراتها إلى الأفراد في هذه المرة عن طريق نشرها على صفحات الإنترنت، وكذلك تحصيل الضرائب وغيرها من الإيرادات من الأفراد وإنهاء المعاملات المختلفة عن طريق تلك المواقع التي تخصها، ولكن ما يزال هذا القسم محدود الانتشار، ولكنه يتطور بتطور المستويات الأخرى.

- تجارة إلكترونية بين الزبائن والزبائن: من خلال هذا القسم من أقسام التجارة الإلكترونية يستطيع الزبائن العارضين والزبائن الراغبين في الاقتناء أو المبادلة التواصل من خلال منطقة حرة إلكترونية تسمح لهم بذلك مثل موقع (Ebay).

خصائص التجارة الإلكترونية:

تتميز التجارة الإلكترونية بطبيعتها بمجموعة من الخصائص والتي تميزها عن التجارة التقليدية وهذه الخصائص هي:

1. عدم وجود علاقة مباشرة بين طرفي العملية التجارية حيث يتم التلاقي بينهما عن طريق شبكة الاتصالات ، ويتميز هذا الأسلوب بوجود درجة عالية من التفاعل بغض النظر عن وجود الطرفين في نفس الوقت على الشبكة.
2. عدم وجود أي وثائق ورقية متبادلة في إجراء وتنفيذ المعاملات ، حيث كافة عمليات التفاعل تتم بطريقة إلكترونية ، ودون استخدام أي أوراق.
3. إمكانية التفاعل مع أكثر من مصدر في الوقت نفسه، حيث يستطيع أحد الأطراف إرسال رسالة إلكترونية إلى عدد لا نهائي من المستقبلين في نفس الوقت

وبذلك تتوفر إمكانات بلا حدود للتفاعل الجمعي أو المتوازي وهو شئ غير مسبوق.

4. إمكانية تنفيذ كل مكونات العملية التجارية. بما فيها تسليم السلع غير المادية على الشبكة وذلك بخلاف أي من وسائل الاتصال السابقة.

5. توفر في النفقات الإدارية ونفقات الاتصال وغيرها، حيث تعتبر بديلاً عن تخصيص جزء كبير من رأس المال في إقامة علاقات مستمرة بين البائعين والمشترين، كما أنها تسمح بإتمام عملية التوزيع رأساً للمستهلك.

6. تعتبر ذات أهمية خاصة لكل من المنتجين والمستهلكين في الدول النامية حيث تمكن من التغلب على الحواجز التقليدية للمسافة ونقص المعلومات عن الفرص التصديرية ([6]).

تحديات التجارة الإلكترونية:

- هناك نقص في الاعتمادية والأمان والمعايير والبروتوكولات.
- أدوات تطوير البرمجيات ما زالت تتغير باستمرار وسرعة.
- تصعب عملية وصل الإنترنت وبرمجيات التجارة الإلكترونية مع بعض التطبيقات وقواعد البيانات المستخدمة.
- احتياج المزودين إلى مزودات خاصة للويب ولبنى تحتية أخرى بالإضافة إلى مزودات الشبكات.
- بعض برمجيات التجارة الإلكترونية لا تتناسب برمجياً وتقنياً مع بعض أنظمة التشغيل.

التحديات غير التقنية للتجارة الإلكترونية:

- الكلفة والتسويق: كلفة تطوير التجارة الإلكترونية بواسطة الشركة بنفسها قد يكون عالياً جداً والأخطاء الناتجة عن قلة الخبرة قد تسبب تعطيل التجارة الإلكترونية. هناك عدة فرص لمنح شركات تقنية بالقيام بهذه المهام ولكن ليس من السهل معرفة أي شركة هي المناسبة. ولتسويق هذا النظام فإن على المدير أن يتعامل مع فوائد غير حسية وهي صعبة الحساب.

- الأمن والخصوصية : هذه الأمور مهمة جداً في عالم الشركة للمستهلك خصوصاً في ميدان الأمن والأمان والتي يظن الكثير من الناس بأنها منيعة 100٪ والكثير من الناس تحجم عن المشاركة في التجارة الإلكترونية بدواعي الخوف من الكشف عن خصوصياتهم.
- انعدام الثقة ومقاومة المستخدم: بعض من الزبائن لا تثق بالباعة المجهولين الذي لا يرونهم ولا يثقون بالمعاملات غير الورقية ولا بالنقد الإلكتروني.

عوامل أخرى:

- انعدام لمس المنتجات فبعض الزبائن يودون لمس المنتجات قبل شرائها.
- الكثير من الأمور القانونية لم يتم حسمها بعد في التجارة الإلكترونية خصوصاً المتعلقة بالقرصنة.
- التجارة الإلكترونية ما زالت في طورها الأول والذي يتميز بالتغير السريع. الكثير من الناس تود أن ترى شيئاً ثابتاً قبل الاستثمار فيه.
- لا يوجد عدد كاف من الباعة والمشترين في الكثير من التطبيقات لجعل هذا الأمل مريحاً.
- التجارة الإلكترونية قد تسبب انهيار في علاقات الناس مع بعضها البعض.
- الدخول على الإنترنت ما زال باهظ الثمن للكثير من الناس وسرعة الاتصال ما زالت بطيئة في الكثير من دول العالم.

الفوائد التي تجنيها الشركات من التجارة الإلكترونية:

تقدم التجارة الإلكترونية العديد من المزايا التي يمكن أن تستفيد منها الشركات بشكل كبير ويذكر منها على سبيل المثال لا الحصر:

- تسويق أكثر فاعلية وأرباح أكثر: إن اعتمادنا على الإنترنت في التسويق يتيح لها عرض منتجاتها وخدماتها في مختلف أصقاع العالم دون انقطاع طيلة ساعات اليوم وطيلة أيام السنة مما يوفر لهذه الشركات فرصة أكثر لجني الأرباح إضافة إلى وصولها إلى المزيد من الزبائن.

- **تخفيض مصاريف الشركات:** تعد عملية إعداد وصيانة مواقع التجارة الإلكترونية على الويب أكثر اقتصادية من بناء أسواق التجزئة أو صيانة المكاتب ولا تحتاج الشركات إلى الإنفاق الكبير على الأمور الترويجية ، أو تركيب تجهيزات باهظة الثمن تستخدم في خدمة الزبائن، ولا تبدو هناك حاجة في الشركة لاستخدام عدد كبير من الموظفين للقيام بعمليات الجرد والأعمال الإدارية ، إذ توجد قواعد بيانات على الإنترنت تحتفظ بتاريخ عمليات البيع في الشركة وأسماء الزبائن ويتيح ذلك لشخص بمفرده استرجاع المعلومات الموجودة في قاعدة البيانات لتفحص تواريخ عمليات البيع بسهولة.
- **تواصل فعال مع الشركاء والعملاء:** تطوي التجارة الإلكترونية المسافات وتعبر الحدود مما يوفر طريقة فعالة لتبادل المعلومات مع الشركاء، وتوفر التجارة الإلكترونية فرصة جيدة للشركات للاستفادة من البضائع والخدمات المقدمة من الشركات الأخرى فيما يدعي التجارة الإلكترونية من الشركات إلى الشركات ([7]).

الفوائد التي يجنيها الزبائن من التجارة الإلكترونية:

- **توفير الوقت والجهد:** تفتح الأسواق الإلكترونية بشكل دائم (طيلة اليوم ودون أي عطلة) ولا تحتاج الزبائن للسفر أو الانتظار في طابور لشراء منتج معين كما ليس عليهم نقل هذا المنتج إلى البيت ولا يتطلب شراء أحد المنتجات أكثر من النقر على المنتج، وإدخال بعض المعلومات عن البطاقة الائتمانية، ويوجد بالإضافة إلى البطاقات الائتمانية العديد من أنظمة الدفع الملائمة مثل استخدام النقود الإلكترونية.
- **حرية الاختيار:** توفر التجارة الإلكترونية فرصة رائعة لزيارة مختلف أنواع المحلات على الإنترنت، وبالإضافة إلى ذلك فهي تزود الزبائن بالمعلومات الكاملة عن المنتجات ويتم كل ذلك بدون أي ضغوط من الباعة.
- **خفض الأسعار:** يوجد على الإنترنت العديد من الشركات التي تبيع السلع

بأسعار أخفض مقارنة بالمتاجر التقليدية، وذلك لأن التسوق على الإنترنت يوفر الكثير من التكاليف المنفقة في التسوق العادي، مما يصيب في مصلحة الزبائن.

- **نيل رضا المستخدم**: توفر الإنترنت اتصالات تفاعلية مباشرة، مما يتيح للشركات الموجودة في السوق الإلكتروني الاستفادة من هذه الميزات للإجابة على استفسارات الزبائن بسرعة مما يوفر خدمة أفضل للزبائن ويستحوذ على رضاهم.

عيوب وسلبيات التجارة الإلكترونية:

لكن ومع هذه الأهمية إلا أنه تبقى هناك عيوب وسلبيات لهذه التجارة ومنها:

1. عدم ثقة المستهلك بدرجة الجودة والتشكيك في مصداقيته للمعارض والمعروض.
2. خطر تمويل أوامر الشراء والتخوف من التلاعبات التي قد تحدث.
3. المشاكل التي قد تنجم من التسوية في مجالي الدفع والاستلام.
4. مستوى الخدمات التي يمكن تقديمها في ظل تزايد وتوسيع شبكة المستهلكين ومدى مقدرة الشركة على تلبية هذه الطلبات التي لن يكون لها زمان أو مكان محددين.
5. سرقة المعلومات التي تعرضها الشركات أو محاولة العبث بها.
6. فقدان متعة التسوق التي يعتبرها العديد من الناس فرصة للترويج وكسر حالة الجمود في حياتهم الروتينية اليومية.
7. مكلفة بعض الشيء بالنسبة للشركات الكبيرة.
8. تحتاج إلى جهد كبير بالنسبة للمتاجرة الكبيرة أمثال (ZDNET) وأمازون ([8]) .

وتبقى التجارة الإلكترونية كغيرها من التجارب والممارسات بحاجة إلى وقت لتأكيد دورها وإبراز إيجابياتها، والعيوب التي ذكرت من الممكن تلافيها أو على الأقل التقليل منها وذلك باتباع الإرشادات ومراقبة الموقع أولاً بأول.

طرق السداد المباشرة للأموال عبر الإنترنت:

1 - بطاقة الائتمان "Credit Card":

هذه البطاقات تصدر عن بنك تجاري، لا يوجد فيه حساب لحامل البطاقة "وسيلة ائتمان"، ويقوم البنك المصدر بسداد قيمة التعاملات الإلكترونية التي تم دفع قيمتها بواسطة تلك البطاقة التي أصدرها، ويقوم البنك المصدر للبطاقة بإرسال فاتورة شاملة مصنفة للعميل حسب المعاملات التي قام بإجرائها، ويطالبه بسداد جزء يسير من قيمة تلك المعاملات قريب من 5٪.

ويقوم البنك المصدر بزيادة رصيد البطاقة على المبلغ الذي في ذمته بنسبة معلومة شهرياً تصل إلى1.5٪ وهو ما يسمى بتدوير الائتمان، وهذه البطاقة تتفاوت في المزايا التي تقدمها لحاملها، ولذلك تجد البنوك التجارية تصنفها حسب المزايا، فتجعل أقل المزايا للنوع التقليدي "الكلاسيكي -الفضي" والنوع الذي بعده هو النوع الذهبي والذي بعده البلاتيني أو الخاص برجال الأعمال.

وأهم المزايا التي تتفاوت فيها هذه البطاقة هي ميزة السقف الائتماني الممنوح لحامل البطاقة، وفي حالة العملاء غير المؤهلين ائتمانياً للحصول على بطاقة ائتمانية تقوم بعض البنوك بمطالبة العميل بإيداع رهنا مقابل عمليات البطاقة ويسمى هذا النوع "بالطاقات الائتمانية المضمونة".

وتحتوي بطاقة الائتمان على بيانات مثل اسم العميل صاحب تلك البطاقة وكذلك تاريخ انتهائها وأما الأهم فهو رقم البطاقة وهو رقم سري لا يعرفه سوى الجهة المصدرة "البنك" وصاحب البطاقة.

ولا تستخدم تلك البطاقة فقط في التسديد عبر الإنترنت لقيمة المعاملات الإلكترونية التي تحدث من خلال تلك الشبكة، بل وتسديد قيمة المعاملات التي تجري على أرض الواقع، وفي أي مكان يقبل بهذه البطاقة.([9])

ومن أشهر الشركات المصدرة لهذا النوع من البطاقات شركة "فيزا" وشركة "ماستر كارد"، ويتم إصدار تلك البطاقات عبر البنوك التجارية كوسيلة ائتمان كما ذكر سابقاً، وتقوم تلك الشركات بتزويد التقنيات اللازمة لإصدار تلك

البطاقات والتعامل معها لتلك البنوك، ويتم ذلك مقابل رسوم عضوية تدفعها البنوك لتلك الشركات، وتجدر الإشارة هنا الى أن بنك فلسطين يقدم تلك الخدمة الائتمانية منذ عام 1999.([10])

ومع اتساع استخدام تلك البطاقات في تسديد قيمة المعاملات الإلكترونية التي تحدث عبر الإنترنت، قامت كثيراً من البنوك بتقديم خدمة جديدة، وذلك بإصدار فيزا خاصة بالإنترنت فقط، وذلك لتشجيع عملائها على الدخول في عالم التجارة الإلكترونية، بما توفره هذه البطاقات من سرعة وأمان وسهولة في التعامل.

كما وقامت بعض البنوك بإضافة خدمة جديدة إلى هذه البطاقات عن طريق ضمان البنك قيمة صفقات التجارة الإلكترونية إذا لم يتمكن صاحب البطاقة من الحصول على حقه من التاجر الذي تعامل معه.([11])

وتجدر الإشارة هنا أيضاً انه تم في المبحث السابق توضيح لعملية السداد بواسطة الائتمان والدور الذي يقوم به الوسيط المالي في هذه العملية.

2 - النقود الإلكترونية: "ELECTRONIC MONEY"

تعرف شركة (ايرنست أند يونغ) النقود الإلكترونية بأنها مجموعة من البروتوكولات والتواقيع الرقيمة التي تتيح للرسالة الإلكترونية ان تحل فعلياً محل تبادل العملات التقليدية.

وبعبارة أخرى، فإن النقود الإلكترونية أو الرقمية هي المكافئ للنقود التقليدية التي تم الاعتياد على تداولها.

والنقود الإلكترونية على عدة أشكال منها:

- **البطاقات البلاستيكية الممغنطة:**

هي بطاقات مدفوعة سلفاً وتكون القيمة المالية مخزنة فيها، ويمكن استخدام هذه البطاقات للدفع عبر الإنترنت وغيرها من الشبكات، كما يمكن استخدامها للدفع في نقاط البيع التقليدية.

وتجدر الإشارة هنا إلى هذه الآلية لا تنطبق على بطاقات الائتمان، لأن مستخدم

بطاقات الائتمان يقوم بدفع النقود للبنك بعد عمليات الشراء وليس قبلها كما هو الحال مع هذه البطاقات.

حيث يقوم المستخدم سلفاً بدفع مقدار من النقود التي يتم تمثيلها بصيغة إلكترونية رقمية على البطاقة الذكية، وعندما يقوم المستخدم بعملية شراء سواء أكان عبر الإنترنت أم في متجر تقليدي يتم حسم قيمة المشتريات، وهنالك العديد من منتجات النقود الإلكترونية التي يمكن إعادة تحميلها بقيمة مالية عن طريق إيداع نقود في البنك أو عن طريق أي حركة مالية أخرى ملائمة.

- **النقود الإلكترونية البرمجية:**

هي أنظمة برمجية تتيح مكافئا إلكترونيا لا يحتاج إلى بطاقة بلاستيكية فهي أنظمة تعتمد بالكامل على برمجيات لدفع النقود عبر الإنترنت، وكي يكون نظام النقود الإلكترونية المعتمد بالكامل على البرمجيات فعالاً وناجحاً، لا بد من وجود ثلاثة أطراف فيه هي: الزبون أو العميل، المتجر، البائع، والبنك الذي يعمل إلكترونياً عبر الإنترنت "ONLINE-BANK"، وإلى جانب ذلك لابد من أن يتوفر لدى كل طرف من هذه الأطراف برنامج النقود الإلكترونية نفسه، ومنفذ إلى الإنترنت كما يجب أن يكون لدى كل من المتجر والعميل حساب بنكي لدى البنك الإلكتروني الذي يعمل عبر الإنترنت.

- **المحفظة الإلكترونية:**

المحفظة الإلكترونية هي برنامج ينظم عمليات الدفع بواسطة البطاقة الائتمانية إذ تحفظ بيانات البطاقات الائتمانية في صيغ مشفرة على القرص الصلب العائد لصاحب البطاقات، وعند قيام صاحب المحفظة بعمليات شراء عبر الإنترنت من جهات تدعم نوع محفظته الإلكترونية يقوم برنامج المحفظة بتوفير الوقت اللازم لتعبئة بيانات بطاقة الائتمان عند القيام بمعاملة إلكترونية عبر الإنترنت.

فعلى سبيل المثال أنه وفي كل مرة يتم فيها الشراء عبر الإنترنت، يتطلب الأمر إدخال بيانات بطاقة الائتمان وبيانات أخرى مثل العنوان ورقم التليفون وأشياء أخرى.

ففكرة عمل هذه الحافظة بسيطة وهي كتابة تلك البيانات مرة واحدة وعند

القيام بزيارة أي موقع على الشبكة لإتمام أي معاملة وتطلب الأمر في تلك المعاملة الدفع باستخدام بطاقة الائتمان، فإن هذه المحفظة ستقوم بإرسال هذه البيانات أوتوماتيكياً لهذا الموقع.

وتجدر الإشارة هنا إلى ان هذه الحافظة لا تعمل في كل المواقع وبعض الحافظات تعمل في مواقع ولا تعمل في غيرها.

الشيكات الإلكترونية:

الشيك الإلكتروني والمكافئ للشيكات الورقية التقليدية التي اعتاد الناس على التعامل بها، لكنه عبارة عن رسالة إلكترونية موثقة ومؤمنة، أما عن كيفية عمل تلك الشيكات فهي كالتالي:

1. في حالة وجود موقع ويب يمكن إضافة زر ربط في نموذج الدفع أو الفاتورة التي يتضمنها الموقع، بحيث ينقل ذلك الزر إلى نموذج الشيكات الإلكترونية في موقع الوسيط الآمن، في حالة عدم وجود الموقع فلا توجد مشكلة، حيث يمكن وضع الرابط في الرسالة البريدية التي تحتوي على الفاتورة، وبذلك يمكن الاستفادة من هذه الخدمة على الرغم من عدم وجود الموقع.

2. يقوم المشتري بتعبئة نموذج الشراء، أو الفاتورة حيث تعود إلى البائع مباشرة عبر البريد الإلكتروني بعد تعبئتها، في الوقت الذي يحرر شيكاً إلكترونياً لصالح الوسيط الذي يتحقق من صحة المعلومات البنكية، من خلال الاستفسار عبر الشبكة في قاعدة معلومات بنك العميل، فيرسل مباشرة إشعاراً رسمياً للبائع والمشتري بصلاحية العملية.

3. يحرر موقع وسيط الدفع بالشيكات، شيكاً إلكترونياً نيابة عن المشتري ويودعه في حساب البائع مباشرة.

1. يرسل الوسيط إلى البائع كل نهاية شهر، كشفاً بقيمة العمولات المستحقة للوسيط على هذا البائع، ويقبل هذا الوسيط الدفع بالشيكات الإلكترونية ولا تحتسب هذه العمولات كنسب على قيمة العملية مهما كان حجمها، بل كقيمة

ثابتة وليس هناك وقت محدد على معالجة هذه العملية فيمكن أن تحدث خلال أي وقت.([12])

مزايا النقود الإلكترونية:

· تكلفة تداولها زهيدة: تحويل النقود الإلكترونية عبر الإنترنت أو الشبكات أرخص كثيراً من استخدام الأنظمة البنكية التقليدية.

· لا تخضع للحدود: يمكن تحويل النقود الإلكترونية من أي مكان إلى حد كبير فهي تغني عن ملئ الاستمارات وإجراء الاستعلامات البنكية عبر الهاتف.

· تسرع عمليات الدفع: تجري حركة التعاملات المالية ويتم تبادل معلومات التنسيق الخاصة بها فوراً في الزمن الحقيقي دون الحاجة الى أي وساطة، مما يعني تسريع هذه العملية.

· تشجيع عمليات الدفع الآمنة: تستخدم البنوك التي تتعامل بالنقود الإلكترونية أجهزة خادمة تدعم بروتوكول الحركات المالية الآمنة "SET"، كما تستخدم مستعرضات لشبكة الويب تدعم بروتوكول الطبقات الأمنية "SSL"، مما يجعل عمليات دفع النقود الإلكترونية أكثر أماناً.([13])

وسوف يتم تناول البروتوكولات الأمنية السابقة وغيرها من المفاهيم التي تعلق بموضوع الأمن المرتبط بالمعاملات الإلكترونية في هذا المبحث.

الجوانب الأمنية للتجارة الإلكترونية:

واقع النظام الأمني المطبق عبر شبكة الإنترنت:

عندما تم تصميم الإنترنت "أو على الأقل الشبكة التي أصبحت بالفعل الإنترنت" لم يتوقع مخترعوه أن كثيراً من الناس سيقومون باستخدام ذلك النظام أو أنهم سيستخدمونه بهذا الشكل الذي هو عليه اليوم، وعلى الرغم من البدايات العسكرية للإنترنت، فإنها لم تصمم لتكون شبكة آمنة، فعلى الإنترنت يمكن لأي فرد أن ينصت إلى أي معلومة ترسل عبر الشبكة، سواء كانت مرسلة بالبريد الإلكتروني أو من وإلى موقع شبكة الويب، إلا أن ذلك قد يعد مشكلة كبيرة عندما يكون متعلقاً

بالمعلومات أو الشخصية.

وبالطبع فإن مثل تلك المعلومات هامة جداً لإتمام المعاملات سواء ما يتعلق منها بالتجارة الإلكترونية أو غيرها والتي تحدث عبر الإنترنت حيث أنه في كثير من الأحيان تتطلب تلك المعاملات تبادل معلومات شخصية مهمة ، كرقم بطاقة الائتمان والحساب الصرفي، وكذلك ما يتم نقله بواسطة البريد الإلكتروني مثل العقود الموقعة والوثائق والتي تحتوي في معظم الأحيان على معلومات خاصة أو سرية ولذلك فإن (56٪) من متصفحي الإنترنت يعزفون عن إتمام معاملات الشراء على الإنترنت ، وفي الجانب الآخر من المعاملة التجارية تخاف الشركات من تقديم المستخدمين لطلبات تعويض مزيفة، ومن عدم تسديد قيمة المشتريات وما إلى ذلك ولذلك فإنه ليس مستغرباً أن تشير نتائج استبيان أجري مؤخراً إلى نسبته (42٪) ممن شملهم ذلك الاستبيان يضعون عامل الأمان في المرتبة الأولى، بينما وضع (18٪) عامل الخصوصية في المرتبة الأولى ، وفي دراسة أخرى حديثة، نشرت نتائجها أن (80٪) من المواقع التجارية معرضة للاختراق بسبب قصور الإجراءات الأمنية بها، والناتجة عن أخطار برمجية نتيجة لعدم تحديث أنظمة تحديث أنظمة التشغيل بها أو أخطار بشرية لعدم معرفة مديري الشبكات بالطرق الفنية الصحيحة لتركيب الأنظمة والخدمات وتحديد الصلاحيات.

إن عمليات الاقتناص لأرقام الحسابات وبطاقات الائتمان والتخريب في المواقع ونشر المواقع الكاذبة وغيرها من الجرائم التي تحدث عبر شبكة الإنترنت والتي تسمى بالجرائم الإلكترونية ، قد أصبحت تكلف باهظاً حيث بلغت خسائر عمليات النصب على بطاقات الائتمان وحدها، إلى ما يقرب من (400) مليون دولار خلال أحد الأعوام القليلة الماضية كما إصلاح الأضرار التي ألحقتها الفيروسات التي تصيب أجهزة الكمبيوتر حول العالم قرابة (21) مليار دولار، ولقد دفعت مثل هذه الأرقام وغيرها (30) دولة إلى توقيع الاتفاقية الدولية الأولى لمكافحة الجريمة عبر الإنترنت في بودابست ، وتشكل تلك المعاهدة أول أداة قانونية ملزمة للدولة في إطار مكافحة الجريمة الإلكترونية ، وقد بدأت الولايات المتحدة الأمريكية تنفيذ خطتها الرامية

لتكوين خبراء حماية من الإرهاب الإلكتروني، ولقد بدأت طلائع طلبة من نوع خاص تتكون من 180 طالباً في تلقي دروس مختصة بمكافحة تلك الظاهرة ([14]) .

وتضع الحكومة الأمريكية المهمة المتعلقة بمكافحة الجريمة الإلكترونية من بين أولوياتها، ولقد طلب الرئيس الأمريكي جورج بوش رفع الاعتمادات المخصصة لموضوع مكافحة الإرهاب الإلكتروني إلى (3 -19) مليون دولار بعد أن كان الكونغرس قد وافق على تخصيص مبلغ (11) مليون ([15]) .

إن ما سبق وغيره الكثير يؤكد على أهمية عنصر الأمن وضرورة توفره على تلك الشبكة لحماية ما يوجد عليها وينتقل من خلالها ، وخاصة ما يتعلق بالمعلومات المالية أو الشخصية.

أساليب الاحتيال عبر الشبكة:

هنالك عدة طرق سيحاول بها بعض المجرمين سرقة أو تبديل المعلومات التي تمر من خلاله تلك الشبكة أو توجد على مواقعها والتي من أهمها المعلومات المالية مثل أرقام بطاقات الائتمان والأسماء الموجودة على تلك البطاقات ، وتواريخ استحقاقها "انتهائها" ثم يقوم باستخدام هذه المعلومات فيما بعد لشراء سلع أخرى عبر الإنترنت لتسلم إلى عنوان مؤقت، وبمرور الوقت يتم اكتشاف عملية الغش ويختف المجرمون، ومن أساليب الاحتيال التي يستخدمها هؤلاء المجرمون للقيام بأعمالهم تلك ، أسلوب محاكاة المواقع ، التلصص على المعلومات، تبديل المحتوى الإنكار ([16]) .

1 - أسلوب محاكاة الواقع:

هو تقليد موقع ويب حقيقي بما في ذلك تخطيطه والألوان والوظيفة من أجل الحصول على معلومات بطاقة الائتمان أو سرقة عمل تجاري وتضم هذه الطريقة تسجيل اسم النطاق " عنوان الموقع" وثيق الشبه بموقع مبيعات سليم قانونياً، وربما تختلف في حرف واحد مثل AMAZIN.COM، والخطوة التالية هي تقديم منتج عام بسعر مدهش لحث الناس على إرسال معلوماتهم الائتمانية.

2 - **التلصص على المعلومات:**

هو المصطلح الذي يصف فعل قراءة معلومات غير محمية في أثناء انتقالها عبر أي شبكة، ويتلصص محترفو الشبكة على الرسائل الصادرة والواردة من عناوين مزودي خدمات الإنترنت، وإذا وجودوا شيئاً ما يقومون ببيعه إلى المجرمين والمنافسين.

3 - **تبديل المحتوى:**

من طرق تحويل الأموال المدفوعة يمكن إيقاف رقم الحساب المصرفي وتغييره إلى رقم آخر، وهذا ما يطلق عليه تبديل المحتوى ويستخدمه المتلصصون الذين يستبدلون المحتوى ثم يرسلوا مجموعة جديد من المعلومات إلى مستلمها المقصود أو من المعلومات التي يمكن تبديلها تجد عنوان الشخص الخاص بأية طلبية.

4 - **الإنكار:**

ويقصد بهذا الأسلوب غير القانوني القيام بعمل تجاري مع أية مؤسسة إلكترونياً ثم إنكار حدوث هذه الصفقة أو حتى إنكار البدء فيها، وقد يقوم أحد مستخدمي الإنترنت بطلب منتج على خط ائتماني ثم يشحنه إلى موقع آخر، وعندما يتسلم الفاتورة يذكر المستخدم أنه أصدر أمر بهذه الطلبية الموجودة بالفعل في مخزن مؤجر أو مهجور" ([17]) .

وسائل توفير الحماية على الشبكة:

على الرغم من عدم نظام أمني (100٪) يمنع عمليات القرصنة "الجريمة الإلكترونية" بالكامل حتى في الدول المتقدمة، ولكن استخدام حلول الأمن المتاحة يقلل من حالات الاختراق ويجعل مهمة القراصنة صعبة للغاية، وهناك عدد من الوسائل والطرق التي توفر الحماية من عمليات القرصنة تلك باستخدام المنتجات الحالية والتقنية المتوفرة في السوق، وتعتمد تلك الطرق بالأساس على تقنية التشفير، ولذلك وقبل الانتقال إلى تلك الوسائل والطرق لا بد من ذكر نبذة مختصرة عن تقنية التشفير.

التشفير:

هو عملية الحفاظ على سرية المعلومات (الثابت منها وللتحرك) باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات إلى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك لا يستطيعون فهم شئ لأن ما يظهر لهم هو خليط من الرموز والأرقام والحروف الغير مفهومة، ولقد تحولت عملية التشفير مع انتشار عمليات تبادل البيانات عبر الإنترنت إلى علم واسع يعتبر من الدعائم الرئيسية للتجارة الإلكترونية عبر الإنترنت التي اكتسبت ثقة المستهلك وحازت على اطمئنانه كنوع جديد من التعامل المالي، بفضل وجود وتطر هذا العلم.

كيفية عمل تقنية التشفير:

تتألف عملية التشفير من ثلاثة عناصر هي:

- معادلة التشفير: التي ستطبق على المعلومات لتحويلها إلى بيانات مهمة ومعادلة فك التشفير التي تعيد هذه البيانات إلى حالتها المفهومة الأصلية، ويزداد عامل الأمان الذي توفره هذه المعادلات بازدياد تعقيدها حيث يكون فكها أو استنتاجها صعباً للغاية.
- المفتاح: وهو سلسلة أو أكثر من الرموز تتسلمها المعادلات المتبعة وتطبقها على البيانات لتشفيرها أو فك التشفير عنها ([18]) .

تتبع أنظمة التشفير أسلوبين مختلفين تبعاً للمفاتيح المستخدمة:

أولاً: تشفير المفتاح السري "التشفير المتناظر":

يستخدم هذا النظام المفتاح ذاته في عمليتي التشفير وفك التشفير ويعتمد مبدأ هذا النوع على اتفاق الطرفين المرسل والمستقبل للمعلومات المشفرة على مفتاح سري واحد، ويعتبر عامل أمان هذا النوع أضعف من عامل أمان تشفير المفتاح العام، لأنه قد يتعرض ذلك المفتاح للكشف خلال عملية تبادله بين المرسل والمستقبل عبر الشبكة.

ثانيا: نظام المفتاح العام "التشفير غير المتناظر":

يستخدم هذا النظام زوجاً من المفاتيح: أحدهم يدعى المفتاح العام ويتم الإعلان عنه لجميع الجهات التي تتبادل المعلومات، وهو المفتاح المستخدم لتشفير البيانات والآخر يدعى المفتاح الخاص وهو المستخدم لفك التشفير ويبقى المفتاح سراً عند الجهة المستقبلة، فتزول بذلك ضرورة تبادل المرسل والمستقبل المفتاح والذي يضعف من حماية الأسلوب الأول في التشفير ([19]) .

الوسائل والطرق المستخدمة في توفير الحماية على الشبكة:

1 - **الشهادة الرقمية** : وهي وثائق إلكترونية تصدرها الجهة ذات الصلاحية وهي تتيح التحقق من هوية الشركة صاحبة الموقع التجاري على الشبكة المراد الشراء منه، وذلك عن طريق التأكد من المفتاح العام الخاص بها، حيث تقوم تلك الجهة بمقارنة ذلك المفتاح مع المفتاح الخاص الذي يوجد لديها، فإذا تطابقا سترسل تلك الجهة بالشهادة بالرقمية الخاصة بهذا الموقع، وتلك الجهة ذات الصلاحية بإصدار الشهادات الرقمية تكون جهة محايدة موثوقاً بها، حيث أنها تقبل من المواقع التجارية المفتاح العام، واثبات هواياتهم وتكون أمينة عليهما، وتلك الجهة عادة ما تكون شركات الحماية التي تم ذكرها سابقاً والتي من أمثلتها شركة VERISIGN ، وبالرجوع إلى تجربة الشراء من موقع نايل كوميرس.

2 - **توفيق الرقمي:** هو أسلوب أمني يتيح التأكد من الهوية الخاصة يرسل الرسالة، حيث يقوم المرسل بتشفير الرسالة مستخدماً مفتاحه الخاص، ويقوم المستقبلون بفك التشفير مستخدمين المفتاح العام للمرسل، وإذا نجحت عملية فك التشفير فإن ذلك يعني أن صاحب المفتاح الخاص هو الذي أرسل الرسالة فعلاً.

3 - **البصمة الإلكترونية للرسالة:** هي بصمة رقمية يتم اشتقاقها وفقاً لخوارزميات معينة يطلق عليها اسم اقترانات النمو، ويمكن استخدام هذا الأسلوب للتأكد من أنه إذا حصل أي تخريب أو تعديل في الرسالة فهذا يعني أن الرسالة والبصمة المرافقة لها لن تتطابقا معاً.

4 - **البروتوكولات الأمنية:** لقد استخدمت الشركات الرائدة عالمياً تقنية التشفير لتطوير العديد من البروتوكولات الأمنية ومن أشهر هذه البروتوكولات وأكثرها انتشاراً في الإنترنت واستخداماً في عمليات التجارة الإلكترونية : ([20])

أ - بروتوكولات الطبقات الأمنية:

طورت شركة نتسكيب بروتوكول الطبقات الأمنية بغرض ربط آمن يضمن خصوصية نقل المعلومات بين طرفي الارتباط ، وفي العادة لا تنجز الحركات المالية بواسطة هذا البروتوكول، وإنما يقتصر دوره على نقل المعلومات المتعلقة بها بصورة مشفرة، مثل رقم بطاقة الائتمان وتاريخ انتهائها ، وهذه التقنية عبارة عن برنامج به بروتوكول تشفير متخصص لنقل البيانات والمعلومات المشفرة بين جهازين عبر شبكة الإنترنت بطريقة آمنة بحيث لا يمكن لأحد من الناس قراءتها غير المرسل والمستقبل وفي نفس الوقت تكون قوة التشفير فيها صعبة وقوية ويصعب فكها، وهي تختلف عن بقية طرق التشفير في شئ واحد ألا وهو عدم الطلب من مرسل البيانات اتخاذ أي خطوات لتشفير المعلومات المراد حمايتها وكل الذي يفعله هو التأكد من استخدام هذا البروتوكول بالقوة.

كيفية عمل هذه التقنية:

يقوم هذا البرنامج بربط المتصفح الموجود على جهاز المستخدم "المشتري" بجهاز الخادم الخاص بالموقع المراد الشراء منه، وهذا طبعاً إذا كان الخام مزود بهذه التقنية أساساً، لهذا فإن الكثير إن لم يكن الغالبية من مواقع التجارة الإلكترونية تشترك لدى شركات الحماية مثل (VERISIGN) التي يوفر خادمها مثل تلك التقنية، (ولكن لا بد للخادم الذي يستضيف موقع البيع أن تكون لديه التقنيات القادرة على الاتصال بخادم الموقع الأمن التابعة لشركة الحماية)، ويقوم هذا البرنامج بتشفير أي معلومة صادرة من ذلك المتصفح الموجود على جهاز المشتري وصولاً إلى جهاز الخادم الخاص بالموقع المراد نقل تلك المعلومات له ([21]) .

خطوات استخدام هذه التكنولوجيا:

تتلخص في ثلاث خطوات وهي:

أولاً: يقوم الموقع بالتقدم إلى إحدى الهيئات المستقلة والتي تصدر شهادة رقمية تثبت صحة هوية الموقع، وبعد التأكد من نشاط وحسن سيرة تلك المواقع المتقدمة بالإضافة لاستكمال بعض المتطلبات الأخرى ذات العلاقة، تقوم تلك الهيئة بإصدار الشهادة الرقمية الخاصة بالموقع، بحيث يدون فيه كل المعلومات الهامة مثل اسم الشركة وتاريخ إصدار الشهادة وتاريخ الانتهاء وكذلك يتم إصدار المفتاح العام والمفتاح الخاص للموقع ويقوم الموقع أيضاً بتأمين جهاز خادم مزود ببرنامج "إس إس ال" ليتم تخزين المفتاح العام للموقع به، وقادر على التعامل مع الخادم الآمن.

ثانياً: عند دخول المشتري "زائر الموقع" للصفحة الآمنة التي يدخل بها البيانات المطلوبة لدفع قيمة طلبية مشترياته، يقوم المتصفح المزود بهذا البرنامج (SSL) بالارتباط بالجهاز الخادم الآمن للموقع ويطلب منه التالي: الشهادة الرقمية، مصدرها، تاريخ انتهائها وكذلك تتم المقارنة بين اسم الموقع على الشهادة مع اسم الموقع في جهاز الخادم، وكل هذه الخطوات تتم بواسطة المتصفح لدى المشتري بالنتيجة في حال عدم المطابقة أو إذا كانت هناك ملاحظات.

ثالثاً: بعد خطوة التأكد من مصداقية الموقع والارتباط بجهاز الخادم الآمن يتم تشفير المعلومات على أساس المفتاح العام لذلك الموقع، ليتم نقلها آمنة دون أي تدخل من المشتري ولا يستطيع أحد سرقة المعلومات أو الاطلاع عليها سوى الموقع المعتمد في الطرف الآخر والذي يملك المفتاح الخاص لفتح وإعادة المعلومات إلى وضعها الطبيعي "ويكون هذا الطرف عادة هو الوسيط المالي" ([22]) .

الاحتياطات التي تتخذها الجهة التي تستقبل المعلومات المشفرة:

"عادة تكون شركات الوساطة المالية" ([23]) .

1. حصر فتح تلك المعلومات المشفرة على عدد قليل من الموظفين الموثوق بهم.
2. يتم توزيع المعلومات بعد فتحها وفرزها إلى الأقسام المتخصصة إلكترونياً بحيث لا يتم إعطاء أي قسم سوى المعلومات التي يحتاجها فعلياً، فمثلاً لا يتم إعطاء رقم

بطاقة الائتمان إلا لقسم المحاسبة لخصم المبلغ ويتم تشفيرها مرة أخرى ولا يمكن لأي شخص أن يطلع عليها.

3. تقوم تلك الجهة بإضافة جميع البيانات الخاصة بالمشتري في بنك المعلومات الخاصة بالموقع وهي محمية بجدران اللهب وكلمات العبور، ولا يمكن لأي شخص غير مخول له بالوصول إليها.

4. تقوم تلك الجهات بعمل عدة مستويات من الصلاحيات للموظفين بحيث لا يمكن لأي موظف الوصول إلى معلومات غير مصرح له بالوصول إليها فمثلاً موظفي في قسم الشحن والتخليص ليس له صلاحيات إلى الوصول إلى معلومات عن رقم الطلبية وتاريخها والعنوان المرسل إليه هذا في حالة أن الشركة صاحبة الموقع قامت بعمل الوسيط المالي.

5. التحكم بالحركة في بعض أقسام تلك الجهة ، فمثلاً لا يسمح بالدخول إلى قسم بنك المعلومات إلا للموظفين المصرح لهم والذين يملكون أرقام سرية للدخول.

6. يتم الاحتفاظ بأرقام بطاقات الائتمان مشفرة في أجهزة مستقلة داخل قسم بنك المعلومات وهي غير مرتبطة بالإنترنت.

7. أي تداول للمعلومات بين الأقسام المختلفة في تلك الجهة لا تحمل رقم بطاقة الائتمان وإن حصل فإنها لا تظهر سوى نوع البطاقة وآخر أربعة أرقام.

8. هناك الكثير من الجهات التي تستقبل تلك المعلومات المشفرة حالياً يتم فيها كل شئ إلكترونياً دون تدخل أو إطلاع من الموظفين على تلك المعلومات الهامة.

ب - بروتوكولات الحركة المالية الآمنة:

لقد طورت مجموعة من الشركات العالمية الرائدة مثل شركتا فيزا أو ماستر كارد، بالتعاون مع شركات أخرى منها مايكروسوفت وأي بي أم ، بروتوكولاً لعمليات الدفع، أطلقت عليه اسم بروتوكول الحركات المالية الآمنة، والغاية من هذا البروتوكول ضمان الحفاظ على أمن البيانات وخصوصيتها وسلامتها

والتحقق من وصولها إلى الجهة المطلوبة أثناء إجراء الحركات المالية عبر شبكة مفتوحة مثل الإنترنت، ويشبه هذا البروتوكول إلى حد كبير - بروتوكول الطبقات الآمنة (SSL) في استناده إلى التشفير والتواقيع الرقمية.

أطراف عملية الشراء وفقاً لبروتوكول الحركة المالية الآمنة (SET) : -

تتضمن عملية الشراء وفقاً لهذا البروتوكول خمسة أطراف هي:

1. حامل البطاقة: وهو شخص لديه حساب بطاقة ائتمانية "لدى فيزا أو ماستر كارد".
2. الجهة المتكفلة بالحماية: وهي الجهة التي تتيح انتقال المعلومات المتعلقة بالحركات المالية من المشتري "حامل البطاقة" إلى الوسيط المالي بشكل آمن.
3. التجار: فهم الشركات والأفراد الذين يعرضون البضائع والخدمات عبر الإنترنت، وكي يتمكن هؤلاء التجار من التجاوب مع الحركات المالية التي يقوم بها الزبائن، لابد من الارتباط بعلاقة مع معالجي عمليات الدفع "مؤسسات مالية معتمدة شركات الوسائط المالية".
4. معالجي عمليات الدفع "الوسطاء الماليون" : وهي المؤسسة المالية التي تزود التجار بالحسابات، وتتولى التحقق من عمليات الدفع التي قام بها الزبائن، بالإضافة إلى التعامل معها ومعالجتها.
5. بوابة الدفع : فهي الجهاز الذي يشغله معالج عمليات الدفع الوسيط المالي ويتولى هذا الجهاز معالجة أوامر الدفع التي يتلقاها من مواقع عبر جهة الحماية والصادرة من حامل البطاقات ([24]) .

كيف يمكن تمييز الموقع الآمن:

الإجابة بسيطة فعند الذهاب لموقع آمن يظهر التالي: ([25])

1. تظهر نافذة تبين أن الموقع المراد الدخول إليه هو موقع آمن سواء كان المتصفح(INTERNET EXPLORER) أو (NES CAPE NAVIGATOR) وتلك النافذة دليل على أن الموقع آمن.

2. وجود أيقونة صغيرة تكون على شكل قفل وتوجد في أسفل الشاشة الخاصة بالمتصفح ، فلو كان هذا القفل غير مغلق، فهذا معناه أن هذا الموقع غير آمن أما إن كان مقفلاً فيكون ذلك الموقع آمن وإن لم يكن فلن تظهر هذه الأيقونة.

3. يبدأ عنوان الموقع الآمن بأحرف (:HTTS) بدلاً من أحرف (:HTTP) حيث يشير الحرف (S) إلى موقع مؤمن (SECURE) حيث أن الخدمة خدمة الأمن تلك مقدمة من خادم ويب آمن، مثل خادم شركة (VERISIGN) الذي يوفر تقنية الأمن تلك، ولهذا يمكن القوم الآن وبفضل التكنولوجيا والتقنية الحديثة التي توفر مستوى عالي من السرية ، أن الشراء المباشر من المحلات ببطاقة الائتمان أكثر عرضة للسرقة والاحتيال من الشراء عبر الإنترنت لأن مسئول المبيعات في المحل إذا لم يكن أميناً بإمكانه أن يسجل رقم البطاقة وتاريخ انتهائها واستخدامها في أي وقت يشاء بكل سهولة ، لكن على الإنترنت فالأمر أكثر صعوبة، وتحتاج لأشخاص مختصين يتربصون بواحد من مستخدمي الشبكة ويحتاج الأمر منهم حل أنظمة التشفير المستخدمة، لذا تصبح التجارة الإلكترونية أكثر أمناً من التجارة العادية باستخدام بطاقة الائتمان، لكن السؤال هنا الذي يطرح نفسه، ماذا لو كانت عملية الاحتيال من الشركة (الموقع البائع) نفسها؟ فكيف يمكن التصرف لعدم ضياع حق المشتري أو المتعامل؟

في حال حدوث الاحتيال من قبل الموقع البائع:

هناك الكثير من الممكن أن يفعله المجني عليه حتى يسترد حقه ومن أمثلة ذلك: ([26])

1. مخاطبة الشركة (صاحبة الموقع) التي خدعته: فيجب أن يكون أول شئ يقوم به ذلك المشتري مخاطبة الشركة التي قامت بالنصب عليه وبسرعة، حيث سيكون الدفاع عن ذلك الحق أكثر صعوبة في الانتظار طويلاً قبل المخاطبة، ويجب تجهيز كل المعلومات الخاصة بشكواه قبل الاتصال بتلك الشركة ومن أمثل تلك المعلومات:

•كل المعلومات المتعلقة بعملية الشراء "اسم المنتج – ثمنه – تاريخ ووقت الشراء" وأي معلومات أخرى يمكن أن تكون مفيدة.

•كتابة شكوى عبارة عن فقرة يصف فيها ذلك المشتري ما حدث له.

•في حالة قيام أحد بصرف الشيك الذي دفعه المشتري، أو تم السحب من بطاقته الائتمانية فيجب توفير هذه المعلومة، عند تجهيز ذلك يجب الاتصال بالشركة والتحدث إلى شخص مهمته بحث شكوى العملاء.

2. مخاطبة الشركة التي أصدرت كارت الائتمان الخاص بالمشتري "مثل فيزا" حيث أنه في حالة التعرض لحالة نصب على الإنترنت، وتم الدفع باستخدام كارت الائتمان فستدفع الشركة لذلك المشتري ما خسره ما عدا الخمسون دولاراً الأولى وبعضها كامل المبلغ بعد أن تقوم أغلب الشركات بالتحقق من الشكوى أولاً والتحقق من صحتها.

3. الشكوى لهيئات حماية المستهلك ، فلو تم التعرض لعملية نصب على الإنترنت ولم يحصل ذلك المشتري على نقوده ، يمكنه الشكوى إلى العديد من الهيئات الحكومية والخاصة بحماية المستهلك، حتى يمكنه استرداد تلك النقود، حيث يمكن لتلك الهيئات تعقب المحتالين وإغلاق مواقعهم ومقاضاتهم.

4. القيام بعرض الشكوى في مناطق المناقشة في الموقع المحتال، ومن المتوقع أن يقلل الموقع من تلك الشكوى، لكن يجب تكرار المحاولة ، وكذلك الذهاب إلى واحد من أكثر المواقع شعبية وهو YAHOO لأنه لديه مكاتب للرسائل والمناقشة يشترك فيها الناس من جميع أنحاء العالم وإخبار العالم بتلك التجربة. وهذا الأسلوب ربما لن يعيد نقود ذلك المشتري ،ولكن لذلك يكون قد حذر الآخرين.

وفي النهاية وعلى الرغم من وجود المخاوف من عمليات القرصنة وما يمكن أن تخلفها إلا أن ذلك لن يتعارض مع حقيقة أن التجارة الإلكترونية باتت أسلوباً مميزاً في عقد الصفقات التجارية الناجحة وتوفير فرص الاستثمار بعيداً عن معوقات التجارة التقليدية المتمثلة في مشاكل منافذ الجمرك والنقل والإجراءات الروتينية الأخرى.

نظام المعلومات التسويقية

Marketing Information system (MTC)

يطلق نظام المعلومات التسويقية على كافة الأفراد والتجهيزات والإجراءات والرسائل المصممة ، لغرض جمع المعلومات وتصنيفها وتحليلها وتقييمها وتوزيعها على مراكز اتخاذ القرار التسويقي التي تحتاج إليها وفي الوقت المناسب.

ويتكون نظام المعلومات التسويقية من مجموعة النظم الفرعية التالية :

السجلات الداخلية للمؤسسة Internal records

فالكثير من مديري التسويق يحتاجون إلى المعلومات التي تتضمنها السجلات الداخلية ،والتقارير الدورية الصادرة عن المؤسسة ، لاستخدامها فيما يتخذونه من قرارات يومية ، تتعلق بالتخطيط والتنفيذ والرقابة. فمثلا يقوم القسم المحاسبي في المؤسسات بعمل القوائم المالية ، ويحتفظ بسجلات تفصيلية عن المبيعات والتكاليف والتدفقات النقدية .

كذلك يتولى قسم الإنتاج عمل التقارير الدورية عن برامج الإنتاج والشحن و المخزون . كما يقوم مندوبو المبيعات في العادة بإعداد تقارير دورية عن ردود أفعال المنافسين في السوق إزاء كل ما تقوم به المؤسسة من أعمال كذلك يقوم قسم متابعة خدمات العملاء بإعداد تقارير دورية عن ردود فعل العملاء وشكاواهم ورضاهم عن أداء الخدمات . ويضاف إلي ذلك ، فإن ما يقوم به قسم من أقسام المؤسسة من دراسات وأبحاث يمكن أن يزود الأقسام الأخرى بالمعلومات المتوافرة ، والنتائج التي تم الحصول عليها . ويستخدم المديرون هذه المعلومات في تقييم الأداء ، والتحري عن المشكلات والبحث عن الفرص المتاحة .

وتتميز المعلومات التي يمكن الحصول عليها من السجلات الداخلية للمؤسسات بانخفاض تكلفة الحصول عليها ، كما أنها متاحة ويتم الحصول عليها بسرعة . ومع ذلك فإن استخدام هذه المعلومات ربما ينطوي على مشاكل على درجة عالية من الخطورة والتعقيد . وذلك بسبب أن هذه المعلومات ربما تكون قد جمعت لأغراض تختلف عن تلك التي يريدها مدير التسويق ، أو ربما كانت قد أعدت وجهزت بشكل

خاطئ . ولهذا ، فإن على مدير التسويق أن يكون واعيا لمثل هذه الأمور ، وان لا يأخذ المعلومات على علاتها ، بل يجب عليه أن يعيد تحليلها وتقييمها ليتأكد من مدى صلاحيتها لاستخدامات إدارته ([27]) .

الاستخبارات التسويقية Marketing Lntelligence

تعرف الاستخبارات التسويقية بأنها المعلومات السرية التي تقوم إدارة التسويق بجمعها عن المنافسين للمؤسسة في السوق ، والتي يجب أن تتصف بالانتظام والاستمرارية . ففي ضوء هذه المعلومات تقوم المؤسسة بتعديل خططها وبرامجها التسويقية . وقد تطورت أهمية هذا النوع من المعلومات مع ازدياد حدة المنافسة ، وزيادة حرص مؤسسات الأعمال على معرفة ما يقوم المنافسون بعمله . وتتبنى المؤسسات الكبيرة نظما متقدمة للمعلومات السرية (الاستخبارات) التسويقية عن منافسيها ([28]) .

مصادر الاستخبارات التسويقية ومنها : -

أ. مراكز التوظيف والموظفون في المؤسسات المنافسة . حيث تعتبر طلبات التوظيف وما تتضمنه من شروط ومؤهلات عملية وعلمية لازمة لشغل الوظائف التسويقية الشاغرة لدى المؤسسات المنافسة مصدرا لمعلومات هامة عن اتجاهات تلك المؤسسات . كذلك يعتبر موظفو المؤسسات المنافسة مصدرا هاما للاستخبارات التسويقية . فمن مناقشاتهم وأحاديثهم يمكن للمؤسسة استفاء الكثير من المعلومات .

ب. موظفو المؤسسة أنفسهم من مديرين ومهندسين وعلماء وباحثين يمكن أن يكونوا كلهم قنوات معلومات ، ومصادر هامة للتغذية العكسية المستمرة والمنتظمة إلى مؤسستهم عن كل ما يجري من البيئة ، وما يقوم به المنافسون من ردود أفعال وممارسات .

ج. الأفراد والمؤسسات اللذين يتعاملون مع المنافسين . ويعتبر عملاء المؤسسة مصدرا هاما لهذه المعلومات .

د. التقارير والمعلومات المنشورة . وإن هذه المعلومات والمواد الإعلامية المنشورة عن المؤسسات المنافسة تمثل مصدرا في غاية الأهمية . فالتقارير تبوح بما تقوله

المؤسسات عن نفسها . فما تنشره الصحافة عن هذه المؤسسات وإنجازاتها واختراعاتها وما تعلن عنه في إعلاناتها ، يمكن أن تزود المؤسسة المنافسة بمعلومات سرية هامة .

ه. ملاحظة تصرفات المنافسين وتحليل الأدلة المادية عن هذه التصرفات ، حيث يمكن للمؤسسة شراء بعض منتجات المؤسسة المنافسة ،ودراسة وتحليل المضمون السلعي لهذه المنتجات ، وتكلفتها الإنتاجية وطرق إنتاجها ، يضاف إلى ذلك أنه يمكن للمؤسسة الاستفادة من تحليل الوضع التنافسي للمؤسسات المنافسة من حيث حصصها السوقية ، وحجم الإنتاج ، ونظم التوزيع التي تستخدمها تلك المؤسسات وأساليب تعاملها مع الموزعين .

و. التقارير والنشرات الدورية التي تصدرها بعض الأجهزة الحكومية المعنية بالنشاط الصناعي والتجاري كوزارة الصناعة والتجارة ، وغرف الصناعة وجمعيات المصدرين ، ومراكز الأبحاث والاستشارات بإصدار الكثير من النشرات والتقارير التي يمكن أن تستفيد منها مؤسسات الأعمال .

وقد عمدت المؤسسات لأجل تعزيز قدراتها التنافسية في الأسواق إلى تحصين نفسها من المؤسسات المنافسة والمحافظة على سرية ما تقوم به من أعمال . كما قامت في الوقت نفسه بإنشاء مكاتب متخصصة لجمع المعلومات التي تنشر عن المؤسسات المنافسة وتحليلها وتوزيعها على الجهات التي تحتاج إليها داخل المؤسسة .

والحقيقة أن صانع القرار التسويقي لا يستطيع الاعتماد فقط على ما حصل عليه من معلومات استخبارية ، ولهذا فإنه يحتاج في الغالب إلى دراسات رسمية لأوضاع معينة .

فقد لا يستطيع نظام الاستخبارات التسويقية توفير المعلومات اللازمة ، وهنا يتعين على إدارة التسويق إجراء دراسات تستهدف الحصول على هذه المعلومات . والتي تفيد الإدارة كثيرا من تصميم ووضع الخطط والبرامج والاستراتيجيات التسويقية . وتنطوي عملية بحوث التسويق على تحديد المعلومات اللازمة ، وتصميم طرق ووسائل الحصول على هذه المعلومات وإدارة وتنفيذ عملية جمع المعلومات ، وتحليل النتائج التي يتم الوصول إليها ، ثم توزيع هذه النتائج ومضامينها التطبيقية على الجهات

التي يمكنها الاستفادة منها داخل المؤسسة ([29]) .

وإذا أدركنا حقيقة الديناميكية التي تتصرف بها الأسواق ، وطبيعة التفاعلات التي تحدث بين قواها الرئيسية ، فإننا سنفهم ما تنطوي عليه تلك الديناميكية من حركة وتغيير مستمرين ، مما يفرض على المؤسسة درجة عالية من الاستعداد والاستجابة الفورية لما يمكن أن تحدثه حركة التجدد والتغيير في قوى السوق من تحديات وأثار . ويفرض هذا كله على المؤسسات الحديثة تبني نظام فعال يضمن عملية تدفق مستمرة ومنتظمة للمعلومات .

أن توافر هذه المعلومات يحدد إلى درجة عالية قدرة المؤسسة على الرد والاستجابة لما يجري في السوق من أحداث وتكيفها معها ، وبالتالي دعم بقائهم واستمرارها في دنيا الأعمال . فإن وجود نظم نشطة وفعالة للمعلومات أصبح يمثل لمؤسسة الأعمال الحديثة أحد مقومات نجاحها وبقائها . كما عبر مدير التسويق في إحدى المؤسسات الكبيرة عن هذه الحقيقة بقوله : " إن الإدارة الجيدة لأية مؤسسة تعني إدارة مستقبلها ويعتمد إدارة هذا المستقبل على مدى تبني الإدارة لنظام فعال للمعلومات فيها " .

كذلك أدى اتساع الأسواق المخدومة من قبل المؤسسات ، والتعقيد في عملياتها إلى زيادة الحاجة إلى معلومات أكثر وأفضل . كما ساعد التطور الهائل في تقنيات إنتاج ومعالجة المعلومات وتجهيزها إلى زيادة إمكانيات الاستفادة منها فباستخدام أجهزة ونظم الحاسوب المتطورة استطاعت الإدارة في تلك المؤسسات رفع مستوى جودة المعلومات وبواسطة تلك المعلومات أخذت التجارة الدولية بإحداث نقلة نوعية في عالم التبادل التجاري عبر الشبكات الإلكترونية .

- ارتباط التجارة الإلكترونية بظاهرة العولمة.
- تتزايد أهمية التجارة الدولية الإلكترونية كلما زاد معدل انتشار واستخدام شبكة الإنترنت.
- تفوق التجارة الإلكترونية الموجهة بين التجار ما يزيد عن عشرة أضعاف التجارة الموجهة نحو الأفراد.
- هناك اختلاف بين التجارة الإلكترونية والتجارة التقليدية بعدم وجود علاقة

مباشرة أو وثائق ورقية متبادلة بين أطراف العملية التجارية.

- تمثل قوانين الاستثمار والنظام الضريبي ووسائل انتقال الأموال عبر الحدود وخاصة نظم الدفع وتحويل الأموال بالوسائل الإلكترونية أبرز محددات التجارة الإلكترونية.
- تساهم التجارة الإلكترونية في تخفيض مصاريف الشركات وتواصل فعال مع الشركات والعملاء.
- تساهم التجارة الإلكترونية في توفير الوقت والجهد وخفض الأسعار ونيل رضا المستهلكين.
- إتباع النصائح والإرشادات المتعلقة بعمليات الشراء الإلكترونية يساهم في تقليل فرص القرصنة الإلكترونية.
- تمثل النقود الإلكترونية وبطاقات الائتمان أكثر الوسائط المالية شيوعاً في سداد قيمة التعاملات الإلكترونية.
- من الأساليب الشائعة في القرصنة الإلكترونية أسلوب محاكاة المواقع وتبديل المحتوى.
- تعتمد وسائل حماية التجارة الالكترونية على تقنية التشفير.
- عدم توافر النظام الآمنة في التجارة الإلكترونية وهذا يؤدي إلى مخاوف لدي بعض الشركات في استخدام مثل هذه التجارة الإلكترونية .
- انتشار استخدام التجارة الإلكترونية في الدول العربية سوف يؤدي إلى رفع معدل النمو الاقتصادي .
- يجب تنظيم قوانين ولوائح من قبل الدول العربية لتنظيم عمل التجارة الإلكترونية وممارستها حتى يطمئن المستخدم لها وان الدول هي التي ترعي هذه التجارة .
- عدم وجود متخصصين وعدم توفر الخبرة اللازم بموضوع التجارة الإلكترونية .

الفصل الثالث

النقود الالكترونية

الفصل الثالث

النقود الالكترونية

ما هي النقود الإلكترونية؟

عرّف شركة إيرنست آنديونغ النقودَ الإلكترونية بأنها مجموعة من البروتوكولات والتواقيع الرقمية التي تُتيح للرسالة الإلكترونية أن تحل فعليا محل تبادُل العُملات التقليدية.

وبعبارة أخرى، فإن النقود الإلكترونية أو الرقمية هي المكافئ الإلكتروني للنقود التقليدية التي اعتدنا تداولها .

وتكون النقود الإلكترونية على عدة أشكال، نذكر منها على سبيل المثال لا الحصر:

البطاقات البلاستيكية المُمَغنَطة

هي بطاقات مدفوعة سلفا تكون القيمة المالية مخزّنة فيها،ويُمكن استخدام هذه البطاقات للدفع عبر الإنترنت وغيرها من الشبكات، كما يُمكن استخدامها للدفع في نقاط البيع التقليدية.(Point of Sale- POS)

وتتلخّص آلية عمل البطاقات البلاستيكية فيما يلي :

ملحوظة مهمة جداً :هذه لآلية لا تنطبق على بطاقات التسليف؛ لأن مستخدِم بطاقة التسليف يقوم بدفع النقود للبنك بعد عمليات الشراء وليس قبلها .

يقوم المستخدِم سلفا بدفع مقدار من النقود التي يتمّ تمثيلها بصيغة إلكترونية رقمية على البطاقة الذكية. وعندما يقوم المستخدِم بعملية شراء - سواءً أكان ذلك عبر الإنترنت أم في متجر تقليدي - يتمّ حسم قيمة المشتريات. وهنالك العديد من منتَجات النقود الإلكترونية التي يُمكن إعادة تحميلها بقيمة مالية عن طريق إيداع نقود في البنك أو عن طريق أي حركة مالية أخرى ملائمة .

هنالك أنظمة برمجية تُتيح مكافئا إلكترونيا لا يحتاج إلى بطاقة بلاستيكية فهي أنظمة تعتمد بالكامل على برمجيات مخصَّصة لدفع النقود عبر الإنترنت.

وكي يكون نظام النقود الإلكترونية المعتَمِد بالكامل على البرمجيات فعالاً و ناجحاً، لا بُدّ من وجود ثلاثة أطراف فيه هي: الزبون أو العميل، والمتجر البائع

والبنك الذي يعمل إلكترونياً عبر الإنترنت .(online-bank)وإلى جانب ذلك لا بُدَّ من أن يتوفّر لدى كل طرف من هذه الأطراف برنامج النقود الإلكترونية نفسه ومنفذ إلى الإنترنت، كما يجب أن يكون لدى كل من المتجر و العميل حساب بنكي لدى البنك الإلكتروني الذي يعمل عبر الإنترنت.

وبالفعل، فقد أصبح من الممكن -عن طريق استخدام برمجي اتم عينة من أشهرها برنامج e Chash استخدام النقود الإلكترونية لإتمام عمليات الشراء والدفع عبر الإنترنت، كما إن هذه البرمجيات تُتيح إرسال النقود الإلكترونية على شكل مرفق (attachment)في رسالة بريد إلكتروني

النقود الإلكترونية البرمجية

قد تكون المحفظة الإلكترونية بطاقة ذكية يُمكن تثبيتها على الكمبيوتر الشخصي أوتكون قُرصا مَرِنا يُمكن إدخاله في فتحة القرص المَرِن في الكمبيوتر الشخصي ليتمّ نقل القيمة المالية (منه أوإليه) عبر الإنترنت.

وجدير بالذكر أن البطاقة الذكية هي بطاقة بلاستيكية مزوَّدة بشريحة (chip) حوسبية، وهي قادرة على تخزين بيانات تُعادل 500 ضعف ما يُمكن أن تخزنه البطاقات البلاستيكية الممغنطة. وبخلاف ما عليه الحال في النقود الإلكترونية التي تعتمد على البرمجيات فقط، فإنه يُمكن استخدام البطاقات الذكية للدفع عبر الإنترنت وفي الأسواق التقليدية .

الشيكات الإلكترونية (Electronic Checks)

المحفظة الإلكترونية

الشيك الإلكتروني هو المكافئ الإلكتروني للشيكات الورقية التقليدية التي اعتدنا التعامل بها. والشيك الإلكتروني هو رسالة إلكترونية موثَّقة ومؤمَّنة يُرسلها مُصدِر الشيك إلى مستلِم الشيك (حامله) ليعتمده ويقدّمه للبنك الذي يعمل عبر الإنترنت، ليقوم البنك أولاً بتحويل قيمة الشيك المالية إلى حساب حامل الشيك وبعد ذلك يقوم بإلغاء الشيك وإعادته إلكترونياً إلى مستلِم الشيك (حامله) ليكون

دليلاً على أنه قد تمّ صرف الشيك فعلاً. ويُمكن لمستلِم الشيك أن يتأكّد إلكترونياً من أنه قد تمّ بالفعل تحويل المبلغ لحسابه .

مزايا النقود الإلكترونية

•تكلفة تداولها زهيدة: تحويل النقود الإلكترونية (أي الرقمية) عبر الإنترنت أو الشبكات الأخرى أرخص كثيراً من استخدام الأنظمة البنكية التقليدية .

•لا تخضع للحدود: يمكن تحويل النقود الإلكترونية من أي مكان إلى آخر في العالم، وفي أي وقت كان، وذلك لاعتمادها على الإنترنت أو على الشبكات التي لا تعترف بالحدود الجغرافية، ولا تعترف بالحدود السياسية.

•بسيطة وسهلة الاستخدام: تُسهِّل النقود الإلكترونية التعاملات البنكية إلى حد كبير، فهي تُغني عن ملء الاستمارات وإجراء الاستعلامات البنكية عبر الهاتف.

•تُسرِّع عمليات الدفع: تجري حركة التعاملات المالية ويتم تبادُل معلومات التنسيق الخاصة بها فوراً في الزمن الحقيقي دون الحاجة إلى أي وساطة، مما يعني تسريع هذه العملية.

•تُشجِّع عمليات الدفع الآمنة: تستخدم البنوك التي تتعامل بالنقود الإلكترونية أجهزة خادمة تدعم بروتوكول الحركات المالية الآمنة (Secure Electronic Transactions- SET)، كما تستخدم مستعرِضات لشبكة الويب تدعم بروتوكول الطبقات الأمنية(Secure Socket Layers- SSL) ، مما يجعل عمليات دفع النقود الإلكترونية أكثر أماناً.

طبيعة النقود الالكترونية

نرى من الضروري تقسيم الكلام في هذا الفرع على فقرتين الأولى تعالج الطبيعة القانونية للنقود الالكترونية فيم يتم تخصيص الفقرة الثانية لبحث الطبيعة الواقعية للنقود الالكترونية والتي سوف تحدد نوع الحق الوارد عليها.

أولا :الطبيعة القانونية للنقود الالكترونية

تختلف الأوراق النقدية عن بقية أنواع الأوراق التي تمثل قيمة معينة ويتم التعامل بها فهي تختلف عن الأوراق التجارية والأوراق المالية ولعل جوهر هذا الاختلاف هو إصدار هذه العملة بقانون وطبعها بشكلية معينة تصدر عن البنك المركزي وهو ما يجعلها ملزمة القبول لدى الفرد بحيث لا يستطيع أحد رفضها في التعامل.

إن هذا الاختلاف يثير تساؤلا حول طبيعة القيمة المالية المخزنة الكترونيا ذلك أنها قد تصدر من البنك المركزي وقد تصدر (نظريا) من مؤسسات مالية أخرى وهو ما يجعل عدها نقودا يلزم الأفراد بقبولها في التعامل أمرا محل نظر .

وقد عولجت هذه المشكلة في الولايات المتحدة وفي الاتحاد الأوربي عن طريق منع إصدار النقود الالكترونية أو أي وسائل الدفع الالكتروني إلا من المؤسسات المالية الائتمانية أو تحت إشرافها وهو تقييد لإصدار العملة الالكترونية .

غير أن هذا الحل ليس حلا سليما برأينا ذلك أن إصدار العملة يرتبط مباشرة بالسياسة الاقتصادية التي يجب أن تنفرد الدولة بتقريريها وهو ما لا يمكن مع وجود جهات أخرى لإصدار النقود.

بالإضافة إلى ذلك فإن العملة الالكترونية تستخدم كما رأينا عبر شبكة الكترونية وهو ما يجعلها تتجاوز الجغرافية والتي تحدد النطاق المكاني للسيادة الوطنية فإذا كانت النقود الالكترونية تتجاوز الحدود الجغرافية وتتسم بالطابع الدولي فهي تشكل خطرا على السيادة الوطنية.

إن الحل الأسلم في نظرنا هو وجود تنظيم قانوني دولي لمسألة إصدار العملة الالكترونية لأن هذه العملة كما تقدم من تعريفها وخصائصها ذات طابع دولي لا يمكن حصر التعامل بها داخل حدود دولة معينة.

ثانيا: الطبيعة الواقعية للعملة الالكترونية

إن كون النقود الالكترونية بيانات مخزنة على الحاسب الآلي وهو ما يطرح سؤالا حول كون هذه النقود شيئا ماديا فيكون ملكيته ملكية أي مال مادي أي أنها حقا عينيا أو أن هذه النقود هي أشياء غير مادية تكون الملكية فيها ملكية أدبية أو ذهنية. إن الإجابة على هذا السؤال ينبغي أن تكون مسبوقة ببيان كيفية خزن المعلومات على الحاسب الآلي لأن العملة الالكترونية واحدة من أنماط هذه المعلومات.

إن العملة الالكترونية تخزن على مادة قابلة للتمغنط تتيح تضمين المعلومات فيها عن طريق مغنطة كل نقطة من نقاطها بإمرار تيار كهربائي فيها (23) إذ تتم الاستفادة من قابلية هذه المادة للتمغنط بالاعتماد على نظام الأرقام الثنائية (نظام 0،1) (24) حيث تكون مغنطة نقطة باتجاه عقارب الساعة مثلا ستجعلها تُقرأ في الحاسوب بوصفها الرقم 1 ولكن لو تمت مغنطتها باتجاه معاكس فستقرأ بوصفها الرقم صفر ويتجميع الأرقام الموجودة في عدة نقاط سوف يتكون رمز معين يمثل كتابة أو معلومات بموجب أنظمة معدة تزود بها أجهزة الحاسوب

مما تقدم نلاحظ أن العملة الالكترونية هي تمثل مادي للقيمة النقدية وبالتالي فإن الحق الوراد عليها هو حق عيني ولا يمنع من ذلك كونها غير قابلة للاستخدام إلا عبر جهاز الحاسوب لأن هذه الصفة تنافي قابلية الرؤية للعملة الالكترونية ولكنها لا تنافي ماديتها

الفرع الثاني: مدى كفاية النقود الالكترونية للوفاء بالالتزامات

يمكن القول بأن هذه المشكلة هي أهم المشاكل التي تنشأ عن استخدام العملة الالكترونية في إطار المعاملات المالية لأن الغرض من النقود بصورة عامة هو الوفاء بالالتزامات تترتب على الأشخاص عن طريق نقل ملكية النقود. فهل تكفي النقود الالكترونية للوفاء بالالتزامات المالية مثلها مثل النقود وتطبق عليها نفس أحكام النقود الورقية ؟

إننا نرى أن النقود الالكترونية هي مرحلة جديدة من مراحل التعامل الإنساني المالي الذي بدأ باستخدام المقايضة وسيلة للحصول على السلع والخدمات ثم ما لبث

أن تحول الإنسان إلى استخدام الذهب والفضة بوصفهما مقياسا لقيمة الأشياء قبل أن تصدر المسكوكات المعدنية التي مثلت المرحلة الأولى من مراحل ظهور العملة التي تطورت لتصبح أوراقا نقدية مطبوعة بشكلية معينة يقوم على أساسها قيمة الأشياء

إن هذا التطور التاريخي يعبر عن حقيقة مهمة هي أن النقد بصورة معينة ليس له قيمة في حد ذاته بل هو رمز لقيمة معينة يتسالم الأفراد على مساوته بها والدليل على ذلك أن صدور قانون بإلغاء عملة معينة أو تغيير شكلها سوف يسلب من العملة القديمة القيمة التي كانت ترمز لها

وما دامت العملة رمزا لقيمة محددة يكون القانون هو الفيصل في تحديدها فيمكن أن يكون هذا الرمز مسكوكة معدنية ويمكن أن يكون ورقة نقدية تطبع بشكل معين كما يمكن أن يكون مجموعة من البيانات المخزنة الكترونياً.

وهذا لا يعني أن تكون هذه النقود شيئا مختلفا عن النقود الورقية أو المعدنية بل هي رمز لشيء واحد هو القيمة المالية وبالتالي فإن قيام المدين بالوفاء بأي منها سوف يكون مبرئا لذمته ولن يعد هنا الوفاء وفاءا بمقابل.

كما يترتب على ذلك أيضا أن ملكية النقود الالكترونية تنتقل بالتسليم وهو تسليم مادي وليس تسليما معنويا لأن الفيصل في التفرقة بين نوعي التسليم هو قيام الموفي بعمل مادي ولا شك أن تسليم النقود الالكترونية يتم بعمل مادي هو نقل البيانات التي ترمز للقيمة المالية من حيازة شخص إلى آخر.

لكن التعامل بالنقد الالكتروني يحتاج إلى تهيئة تنظيم قانوني للمصارف التي تتعامل به إذ ((تخفي عوالم البنوك الالكترونية وتحديدا مشاكل الدفع والوفاء بالالتزامات ومشاكل تقديم الخدمة وما تثيره من مسؤوليات حزمة معتبرة من المشكلات والنزاعات المتوقعة تتطلب جاهزية تتفق مع مخاطرها))

لقد تبين لنا من خلال الموضوع أن النقود الالكترونية هي عبارة عن قيمة نقدية بعملة محددة تصدر في صورة بيانات الكترونية مخزنة على كارت ذكي أو قرص صلب بحيث يستطيع صاحبها نقل ملكيتها إلى من يشاء دون تدخل شخص ثالث.
ولقد قمنا بالتمييز بين النقود الالكترونية وبين بقية وسائل الدفع الالكترونية وذلك

الفرق القائم على أساس وجود شخص ثالث يتدخل في بقية وسائل الدفع الالكترونية.

ثم بينا خصائص النقود الالكترونية التي تتمثل بدفعها عبر شبكة الكترونية وما يترتب على ذلك من تجاوز النقود الالكترونية للحدود الجغرافية، وتتمثل بوجوب توفر نظام مصرفي معد لغرض التعامل مع النقود الالكترونية.

ثم تطرقنا إلى الآلية التي يتم بها التعامل بالنقود الالكترونية وقد تبين لنا كيف أن هذه الآلية تقوم على ثنائية الأطراف لا على ثلاثية الأطراف كما هو الحال في بقية أنواع الوسائل الوفاء الالكتروني.

كما تطرق البحث إلى المشاكل القانونية التي تنشأ من التعامل بالنقد الالكتروني وتمثلت في تحديد طبيعة النقود الالكترونية سواء كانت الواقعية أو القانونية ومدى كفاية النقود الالكترونية للوفاء بالالتزامات.

وبعد دراسة الموضوع توصلنا إلى النتائج الآتية:

1. إن النقود الالكترونية تمثل انعطافة في تاريخ التعامل الإنساني الذي بدأ بالمقايضة لينتهي إلى ترميز القيمة المالية في بيانات مخزنة الكترونيا وهذا النمط يحتاج إلى النظر إلى المفهوم الوظيفي للنقود لا إلى المفهوم الماهوي فالنقود رمز لقيمة مالية تقاس على أساسها قيمة السلع والخدمات وليس ضروريا أن تكون بماهية معينة فيمكن أن تكون ورقا أو معدنا أو بيانات الكترونية.

2. إن النقود الالكترونية تحتاج إلى اعتراف قانوني حتى يمكن عدها نقودا بالمعنى القانوني لكن هذا الاعتراف يجب أن يأتي في إطار تنظيم قانوني دولي لأن هذه النقود كما تبين عند بحث خصائصها ذات طبيعة دولية لا يمكن السيطرة على التعامل بها في إطار الحدود الجغرافية لدولة معينة.

3. إن الحق الوارد على النقود الالكترونية حق وارد على شيء مادي ولا يمكن أن يكون شرط وجود الحاسوب للتعامل بها مانعا من ذلك لأن وجوب التعامل عبر شبكة الكترونية لا ينفي ماديتها.

4.إن النقود لا تعد شيئا مختلفا عن النقود الورقية أو المعدنية فهي رموز لقيمة واحدة وبالتالي لا يعد الوفاء بها إلا دفعا لمبلغ نقدي محدد يبرئ ذمة دافعه ولن يكون وفاءا بمقابل .

أشكال النقود الإلكترونية

تختلف صورة النقود الإلكترونية وأشكالها تبعاً للوسيلة التي يتم من خلالها تخزين القيمة النقدية،وكذلك وفقاً لحجم القيمة النقدية المخزونة على تلك الوسيلة التكنولوجية. فهناك إذاً معيارين لتمييز صور النقود الإلتكرونية: معيار الوسيلة ومعيار القيمةالنقدية.

أولاً: معيار الوسيلة:

نستطيع أن نقسم النقود الإلكترونية وفقاً للوسيلة المستخدمة لتخزين القيمة النقدية عليها إلى البطاقات سابقة الدفع، والقرص الصلب، وأخيراً الوسيلة المختلطة.

– **1-البطاقات سابقة الدفع**:Prepaid Cards ويتم بموجب هذه الوسيلة تخزين القيمة النقدية على شريحة إلكترونية مثبتة على بطاقة بلاستيكية. وتأخذ هذه البطاقات صوراً متعددة. وأبسط هذه الأشكال هي البطاقات التي يسجل عليها القيمة النقدية الأصلية والمبلغ الذي تم إنفاقه، ومن أمثلتها البطاقات الذكية Smart Cardsالمنتشرة في الولايات المتحدة الأمريكية، وبطاقة دامونت سابقة الدفع والتي يتم تداولها بصورة شائعة في الدانمارك. وهناك أيضاً بعض البطاقات التي تستخدم كنقود إلكترونية وتستعمل في ذات الوقت كبطاقات خصم مثل بطاقات المنتشرة في . وهناك أخيراً بطاقات متعددة الأغراض، أي تستخدم في ذات الوقت كبطاقة خصم، وكبطاقة تليفون وكبطاقة شخصية بالإضافة إلى كونها نقوداً إلكترونية.

– **2-القرص الصلب** :ويتم تخزين النقود هنا على القرص الصلب للكمبيوتر الشخصي ليقوم الشخصب استخدامها متى يريد من خلال شبكة الإنترنت ولهذا فإنه يطلق على هذا النوع من النقود أيضاً مسمى النقود الشبكية. وطبقاً لهذه الوسيلة

فإن مالك النقود الإلكترونية يقوم باستخدامها في شراء ما يرغب فيه من السلع والخدمات من خلال شبكة الإنترنت، على أن يتم خصم ثمن هذه السلع والخدمات في ذات الوقت من القيمة النقدية الإلكترونية المخزنة على ذاكرة الكمبيوتر الشخصي.

– 3-**الوسيلة المختلطة** :وتعد هذه الوسيلة خليطاً مركباً من الطريقتين السابقتين، حيث يتم بموجبها شحن القيمة النقدية الموجودة على بطاقة إلكترونية سابقة الدفع على ذاكرة الحاسب الآلي الذي يقوم بقراءتها وبثها عبر شبكة الإنترنت إلى الكمبيوتر الشخصي البائع السلع والخدمات.

خصائص النقود الإلكترونية

من خلال عرضنا السابق، فإننا نستطيع أن نستنتج مجموعة من الخصائص التي تميز النقود الإلكترونية والتي نعرضها في السطور الآتية.

أولاً :النقود الإلكترونية قيمة نقدية مخزنة إلكترونياً: فالنقود الإلكترونية وخلافاً للنقود القانونية عبارة عن بيانات مشفرة يتم وضعها على وسائل إلكترونية في شكل بطاقات بلاستيكية أو على ذاكرة الكمبيوتر الشخصي وذلك كما أوضحنا سالفاً.

ثانياً :النقود الإلكترونية ثنائية الأبعاد:

إذ يتم نقلها من المستهلك إلى التاجر دون الحاجة إلى وجود طرف ثالث بينهما كمصدر هذه النقود مثلاً. فالنقود الإلكترونية صالحة لإبراء الذمة ووسيلة لدفع أثمان السلع والخدمات دون أن يقتضي ذلك قيام البائع بالتأكد من حقيقة هذه النقود أو من كفاية الحساب البنكي للمشتري كما هو الحال بالنسبة لوسائل الدفع الإلتكرونية، حيث يتأكد البائع من مدى كفاية الرصيد الموجود في حساب المشتري.

ثالثاً :النقود الإلكترونية ليست متجانسة:

حيث أن كل مصدر يقوم بخلق وإصدار نقود إلكترونية مختلفة. فقد تختلف هذه النقود من ناحية القيمة، وقد تختلف أيضاً بحسب عدد السلع والخدمات التي يمكن أن يشتريها الشخص بواسطة هذه النقود .فهذه النقود ليست متماثلة أو متجانسة.

رابعاً :سهلة الحمل:

تتميز النقود الإلكترونية بسهولة حملها نظراً لخفة وزنها وصغر حجمها، ولهذا فهي أكثر عملية من النقود العادية. ويرجع ذلك إلى أنها تعفي الفرد من حمل نقدية كبيرة لشراء السلع والخدمات رخيصة الثمن كالصحيفة أو مشروبٍ أو وجبة خفيفة.

خامساً :وجود مخاطر لوقوع أخطاء بشرية وتكنولوجية:

يلاحظ أن النقود الإلكترونية هي نتيجة طبيعية للتقدم التكنولوجي. وعلى الرغم مما تقدمه هذه التكنولوجية للبشرية من وسائل الراحة والرفاهية، فإنها تظل عرضة للأعطال مما يتسبب في وقوع مشكلات كثيرة خاصة في ظل عدم وجود كوادر مدربة وخبيرة تكون قادرة على إدارة المخاطر المترتبة على مثل هذه التقنيات الحديثة.

سادساً :النقود الإلكترونية هي نقود خاصة:

على عكس النقود القانونية التي يتم إصدارها من قبل البنك المركزي، فإن النقود الإلكترونية يتم إصدارها في غالبية الدول عن طريق شركات أو مؤسسات ائتمانية خاصة، ولهذا فإنه يطلق على هذه النقود اسم النقود الخاصة.

المخاطر الأمنية والقانونية للنقود الإلكترونية

إن النقود الإلكترونية بمفهومها السابق، ونظراً لخصائصها المتميزة عن النقود القانونية، قد تثير مجموعة من المخاطر القانونية والاقتصادية والتي تستدعي ضرورة وضع حزمة من الضوابط القانونية التنظيمية لمثل هذه الظواهر الجديدة .وسوف نعرض في هذا الفصل الأهم المخاطر القانونية التي يمكن أن تترتب على التعامل بالنقود الإلكترونية.

المخاطر الأمنية للنقود الإلكترونية

يعد البعد الأمني أحد أهم الموضوعات التي تقلق العاملين في القطاع المصرفي والنقدي. وتمثل النقود الإلكترونية إحدى الظواهر التي يمكن أن تزيد من حجم المخاطر الأمنية. وعلى الرغم من قابلية جميع وسائل الدفع الإلكترونية لإحداث مخاطر أمنية إلا أن النقود الإلكترونية تتمتع بقدرة أكبر على خلق تلك المخاطر والتي من أمثلتها صعوبة التحقق من صحتها، وعدم الاعتراف بها أو عدم قبولها. والجدير بالذكر أن المخاطر الأمنية لا تتعلق بالمستهلك فقط، وإنما قد تمتد أيضاً إلى التاجر وإلى مصدر هذه النقود. فقد تتعرض البطاقات الإلكترونية المملوكة للمستهلك أو للتاجر للسرقة أو للتزييف ويتم معاملتها باعتبارها نقوداً إلكترونية أصلية. وقد يحدث أنيتم التزوير عن طريق تعديل البيانات المخزونة على البطاقات الإلكترونية أو على البرمجيات أو على القرص الصلب للكمبيوتر الشخصي. قد يحدث الخرق الأمني إما كنتيجة العمل إجرامي عمدي مثل التزوير والتزييف وإما كنتيجة لعمل غير عمدي مثل محو أو تخريب موقع من مواقع الإنترنت، وإما الإخلال بتصميمات الأنظمة الإلكترونية و القرصنة الإلكترونية. فمن شأن كل هذه التصرفات والتهديدات السابقة أن تؤدي إلى آثار قانونية وأمنية ومالية خطيرة.

وانطلاقاً مما سبق، فإنه من المهم بمكان أن تتأكد الجهة المصدرة للنقود الإلكترونية من توافر كافة الضمانات الأمنية سواء بالنسبة للمستهلك أو بالنسبة للتاجر وسواء أكان ذلك متعلقاً بالنقود الإلكترونية التي تأخذ شكل البطاقات البلاستيكية أو تلك التي يتم التعامل بها عبر الإنترنت (النقود الشبكية)

من الصعب أن يتوافر الأمان المطلق في الخدمات البنكية الإلكترونية ومع هذا فمن الضروري أن يتناسب مستوى الأمان مع الغرض المطلوب تحقيقه. وعلى هذا فإن الترتيبات الأمنية المتعلقة بالنقود الإلكترونية لابد وأن ترمي بصفة رئيسة إلى تحقيق مجموعة من الأهداف من بينها ضرورة قصر الدخول إلى النظام الإلكتروني للنقود الإلكترونية على الأفراد المسموح لهم فقط، والتأكد من شخصية

جميع الأطراف المعنية وذلك لضمان مشروعية كافة الصفقات المبرمة عبر شبكة الإنترنت.

مخاطر النقود الإلكترونية والسرية (الخصوصية)

إن الممارسة الصحيحة للتعامل بالنقود الإلكترونية تقتضي القدرة على التأكد من أن الصفقات المتبادلة والتي تبرم بواسطة استخدام النقود الإلكترونية تتم فقط بين الأطراف المعنية وأن عملية التبادل تنصب على تلك السلع والخدمات المصرح بها فقط. ومع ذلك يبقى هناك تخوف من قبل المستهلكين وذلك من جراء إمكانية استخدام المعلومات والبيانات المتعلقة بإبرام الصفقات دون ترخيص أو إذن مسبق. وسوف تتضاعف هذه المخاوف مع الازدياد المطرد في استخدام النقود الإلكترونية في إبرام الصفقات التجارية.

إن المحافظة على سرية البيانات المالية الخاصة بجميع الأطراف المتعاملين بالنقود الإلكترونية تعدمن أهم القضايا الشائكة المصاحبة للنمو المتزايد والانتشار الكبير المتوقع للنقود الإلكترونية. فكما هو الحال بالنسبة للمحافظة على سرية الحسابات البنكية للعملاء والتي يحرم بمقتضاها اطلاع أي شخص- غير العميل نفسه - على أحد الحسابات البنكية، فإنه من الضروري أيضاً أن تمنح الأطراف المختلفة المستخدمة للنقود الإلكترونية الضمانات الكافية التي تحد من اطلاع أي طرف آخر غير معنى بالصفقة المبرمة على البيانات المالية المتبادلة عبر شبكة الاتصال. وفي الواقع، إن سرية التعاملات التي تبرم بواسطة النقود الإلكترونية يجب المحافظة عليها من تعدي الآخرين سواء كانوا أفراداً عاديين أو جهات حكومية. وفي تلك الحالة سوف تبرز مشكلة خطيرة ألا وهي التناقض بين ضرورة المحافظة على سرية المعاملات من جهة باعتبارها حقاً من حقوق الأفراد، وحق الدولة في استخدام كافة الوسائل المتاحة للقضاء على الجريمة. على سبيل المثال قد يتعين على الدولة مراقبة شبكات الاتصال المختلفة بهدف الحيلولة دون وقوع جريمة غسيل الأموال أو التهرب الضريبي عبر استخدام النقود الإلكترونية. سيكون من الصعب في مثل هذه الحالات

المواءمة بين المحافظة على سرية و خصوصية معاملات الأفراد من جهة وضرورة مواجهة الجريمة من جهة أخرى.

المخاطر القانونية للنقود الإلكترونية

علاوة على المخاطر الأمنية فمن المتوقع أيضاً أن تثير النقود الإلكترونية بعض المخاطر القانونية.وتنبع هذه المخاطر أساساً من خلال انتهاك القوانين واللوائح مثل جرائم غسيل الأموال، إفشاء أسرار العميل وانتهاك السرية. من ناحية أخرى فإن المخاطر القانونية قد تتولد أيضاً عندما تقنن حقوق والتزامات الأطراف المختلفة المتعاملة بالنقود الإلكترونية بطريقة غير دقيقة. إن العلاقات التعاقدية والقانونية التي تنشأ بين المستهلكين وتجار التجزئة والمصدرين والمشغلين هي علاقات متشعبة ومعقدة.

من المسائل المهمة أيضاً والتي تتعلق بالمخاطر القانونية هي مدى وضوح وشفافية الحقوق والالتزامات الخاصة بكل طرف. فعلى سبيل المثال، سوف تثار مسألة المسؤولية القانونية للأطراف المختلفة في حالات التزييف والتزوير والاحتيال والغش. أخيراً، فإن موضوع حماية المستهلك يعد من أهم المخاطر القانونية التي يمكن أن تفرزها النقود الإلكترونية.من المتوقع أيضاً أن يصاحب انتشار النقود الإلكترونية تزايداً في جرائم التهرب الضريبي حيث سيكون من الصعب على الجهات الحكومية المكلفة بتحصيل الضرائب القيام بربط الضريبة على تلك الصفقات التي تتم بواسطة النقود الإلكترونية نظراً لأن تلك الصفقات تتم خفية عبر شبكة الإنترنت.

وتتلخَّص آلية عمل البطاقات البلاستيكية فيما يلي:

يقوم المستخدِم سلفا بدفع مقدار من النقود التي يتمّ تمثيلها بصيغة إلكترونية رقمية على البطاقة الذكية. وعندما يقوم المستخدِم بعملية شراء -سواءً أكان ذلك عبر الإنترنت أم في متجر تقليدي - يتمّ حسم قيمة المشتريات .وهنالك العديد من منتَجات النقود الإلكترونية التي يُمكن إعادة تحميلها بقيمة مالية عن طريق إيداع نقود في البنك أو عن طريق أي حركة مالية أخرى ملائمة.

هنالك أنظمة برمجية تُتيح مكافئا إلكترونيا لا يحتاج إلى بطاقة بلاستيكية فهي أنظمة تعتمد بالكامل على برمجيات مخصَّصة لدفع النقود عبر الإنترنت.

وكي يكون نظام النقود الإلكترونية المعتَمِد بالكامل على البرمجيات فعالاً وناجحاً، لا بُدَّ من وجود ثلاثة أطراف فيه هي: الزبون أو العميل، والمتجرا لبائع والبنك الذي يعمل إلكترونياً عبر الإنترنت .(online-bank)وإلى جانب ذلك لا بُدَّ من أن يتوفّر لدى كل طرف من هذه الأطراف برنامج النقود الإلكترونية نفسه ومنفذ إلى الإنترنت، كما يجب أن يكون لدى كل من المتجر والعميل حساب بنكي لدى البنك الإلكتروني الذي يعمل عبر الإنترنت.

وبالفعل، فقد أصبح من الممكن - عن طريق استخدام برمجيات معينة من أشهرها برنامج eChashاستخدام النقود الإلكترونية لإتمام عمليات الشراء والدفع عبر الإنترنت، كما إن هذه البرمجيات تُتيح إرسال النقود الإلكترونية على شكل مرفق (attachment)في رسالة بريد إلكتروني.

يتزايد إقبال اليابانيين على استخدام تكنولوجيا "نقدية" جديدة تعرف باسم "النقود الالكترونية"، توفر الوقت اكثر من طرق الدفع المعروفة الاخرى، وتدفع المتسوق للشراء اكثر، وتعمل على الفلسفة المعاكسة لبطاقات الائتمان.

وتوضع بطاقة "النقود الالكترونية" في الهاتف الجوال، وعند استخدامها لدفع عملية شراء ما، فان صاحبها لن يتلقى أي نقود معادة (مثلما هو الحال مع النقود الحقيقية) ولا ينتظر تأكيد دفع او ادخال رقم خاص (كما هو الحال مع بطاقة الائتمان)

وقد ظهرت "النقود الالكترونية" قبل اربع سنوات، ويقدر معهد أبحاث ان 15 مليون شخص على الاقل يستخدمونها حالياً في اليابان، وان الرقم مرشح للوصول الى 40 مليونا (واحد من كل 3يابانيين) بحلول عام 2008.

وقد بدئ استخدام هذه النقود في البداية في القطارات السريعة، واصبحت الآن تقبل في المتاجر الكبرى والمقاهي والمطاعم وأكشاك بيع الصحف ومحلات بيع

الأجهزة الالكترونية، وبذلك لم يعد على المتسوق حمل شيء عدا هاتفه الجوال المزود بالبطاقة الالكترونية.

وتتضمن البطاقات الذكية والهواتف المحمولة التي تزود بها هوائيات استشعار واقراصا صغيرة ذاتدوائر متكاملة تتبع الأدوات المعدة لتسلم ونقلا لأشارات الالكترونية. وعندما يوضع الهاتف قرب السكانر(جهاز المسح) تابع لصندوق الدفع فان الاشارة تنقل ويجري استقطاع النقود الكترونيا.

ويشير المحللون الى ان الفكرة تعمل بشكل جيد في اليابان، بسبب عدم وجود قلق كبير بشأن الأمن والسلامة الشخصية. ففي اليابان غالبا ما تعاد المحافظ المسروقة الى اصحابها بدون المساس بها، ولذلك فان فقدان بطاقة او هاتف جوال به مئات الدولارات من النقد الالكتروني يمثل مخاطرة صغيرة نسبياً.

وتعتمد "النقود الالكترونية" على الزبائن الذين يرغبون في دفع مشترياتهم مسبقا وهي الفلسفة المعاكسة لبطاقة الائتمان. ويطبق هذا في اليابان حيث ينفر السكان من الديون، اذ ان تسعة في المائة فقط من تعاملات المستهلكين تجري بواسطة بطاقة الائتمان

الفصل الرابع

صور الجرائم الالكترونية واتجاهات تبويبها

الفصل الرابع

صور الجرائم الالكترونية واتجاهات تبويبها

يصنف الفقهاء والدارسون جرائم الكمبيوتر والانترنت[1] ضمن فئات متعددة تختلف حسب الأساس والمعيار الذي يستند اليه التقسيم المعني، فبعضهم يقسمها الى جرائم ترتكب على نظم الحاسوب وأخرى ترتكب بواسطته ، وبعضهم يصنفها ضمن فئات بالاستناد الى الأسلوب المتبع في الجريمة، وآخرون يستندون الى الباعث أو الدافع لارتكاب الجريمة، وغيرهم يؤسس تقسيمه على تعدد محل الاعتداء، وكذا تعدد الحق المعتدى عليه فتوزع جرائم الحاسوب وفق هذا التقسيم الى جرائم تقع على الأموال بواسطة الحاسوب وتلك التي تقع على الحياة الخاصة.

ومن الملاحظ أن هذه التقسيمات أو بعضها، لم تراع بعض أو كل خصائص هذه الجرائم وموضوعها، والحق المعتدى عليه لدى وضعها لأساس أو معيار التقسيم.

ان جرائم الكمبيوتر في نطاق الظاهرة الاجرامية المستحدثة، جرائم تنصب على معطيات الحاسوب (بيانات ومعلومات وبرامج) وتطال الحق في المعلومات ويستخدم لاقترافها وسائل تقنية تقتضي استخدام الحاسوب بوصفه نظاما حقق التزاوج بين تقنيات الحوسبة والاتصالات ، ونشير في هذا الصدد الى ان الجرائم التي تنصب على الكيانات المادية مما يدخل في نطاق الجرائم التقليدية ولا يندرج ضمن الظاهرة المستجدة لجرائم الحاسوب.

ولا نبالغ ان قلنا ان ثمة نظريات ومعايير لتصنيف طوائف جرائم الكمبيوتر والانترنت بعدد مؤلفي وباحثي هذا الفرع القانوني ، ومصدر هذا التعدد التباين في رؤية دور الكمبيوتر ومحاولات وصف الافعال الجرمية بوسائل ارتكابها ، ومع هذا وبغض السعي للوقوف على ابرز التصنيفات نعرض لمفهوم ومحل وابرز سمات الجريمة الالكترونية (البند 1) وهذه مسائل لازمة كمدخل لبيان انواعها . ثم ننتقل لبيان نظريات تصنيفها تفصيلا (البند 2) بعد ذلك نعرض بايجاز اوجبته مساحة العرض

[1] ثمة تعدد وتباين في الاصطلاحات الدالة على هذه الجرائم ، عالجناها على نحو واسع في مؤلفاتنا المشار اليها اعلاه وتحديدا كتابنا جرائم الكمبيوتر والانترنت . وكذلم انظر بحثنا " جرائم الكمبيوتر والانترنت المعنى والخصائص والصور واستراتيجية المواجهة القانونية : منشور على موقعنا على الانترنت www.arablaw.org

لمدلول مختلف الانماط التي تتطلب احاطة التشريع بها من ناحية التجريم (البند 3).

1 - تعريف الجرائم الالكترونية ومحلها وابرز سماتها – مدخل

ان الجرائم الالكترونية بادق وصف جرائم تطال المعرفة ، الاستخدام ، الثقة ، الامن الربح والمال ، السمعة، الاعتبار ، ومع هذا كله فهي لا تطال حقيقة غير المعلومات لكن المعلومات – باشكالها المتباينة في البيئة الرقمية – تصبح شيئا فشيئا المعرفة ووسيلة الاستخدام وهدفه ، وهي الثقة ، وهي الربح والمال ، وهي مادة الاعتبار والسمعة . ان جرائم الكمبيوتر بحق هي جرائم العصر الرقمي.

وقد خلت الدراسات والمؤلفات في هذا الحقل (قديمها وحديثها) من تناول اتجاهات الفقه في تعريف جريمة الكمبيوتر عدا مؤلفين ، في البيئة العربية ، مؤلف الدكتور هشام رستم[1] اما في البيئة المقارنة نجد مؤلفات الفقيه Ulrich Siebe[2] اهتمت بتقصي مختلف التعريفات التي وضعت لجرائم الكمبيوتر . وقد اجتهدنا في عام 1994 (في رسالة الماجستير خاصتنا في هذا الموضوع) في جمع غالبية التعريفات التي وضعت في هذا الحقل واوجدنا تصنيفا خاصا لها لمحاولة تحري اكثرها دقة في التعبير عن هذه الظاهرة[3] ، وبغض النظر عن المصطلح المستخدم للدلالة على جرائم الكمبيوتر والإنترنت فقد قمنا في الموضع المشار اليه بتقسيم هذه التعريفات – حتى ذلك التاريخ – الى طائفتين رئيستين : - أولهما ، طائفة التعريفات التي تقوم على معيار واحد ، وهذه تشمل تعريفات قائمة على معيار قانوني كتعريفها بدلالة موضوع الجريمة او السلوك محل التجريم او الوسيلة المستخدمة وتشمل أيضا تعريفات قائمة على معيار شخصي ، وتحديدا متطلب توفر المعرفة والدراية التقنية لدى شخص مرتكبها. وثانيهما ، طائفة التعريفات القائمة على تعدد المعايير ، وتشمل التعريفات التي تبرز موضوع الجريمة وانماطها وبعض العناصر المتصلة باليات ارتكابها او بيئة ارتكابها او سمات مرتكبها . وعاودنا مجددا الوقوف

---

[1] د. هشام محمد فريد رستم ، قانون العقوبات ومخاطر تقنية المعلومات، الطبعة الأولى، مكتبة الآلات الحديثة، اسيوط، 1992. ص 6 و 25 .

[2] مجموعة من المؤلفات ابتداءا من السبعينات آخرها الدراسة الشاملة التي اجراها الفقيه المذكور لمجلس اوروبا حول جرائم الكمبيوتر عام 1998

[3] انظر هذه التعريفات في رسالتنا للماجستير – جرائم الحاسوب ، 1994 ، الجامعة الاردنية.

على مختلف هذه التعريفات وما استجد من تعريفات في السنوات اللاحقة من خلال مؤلفنا جرائم الكمبيوتر والانترنت (2002) ، ودون ان نعود لتفاصيل بحثنا السابق في الموضعين المشار اليهما لعدم ملائمة مقام العرض ، فاننا نكتفي في هذا المقام بايراد خلاصة هذا البحث للوقوف معا على تعريف منضبط يعبر بدقة عن طبيعة وخصوصية ظاهرة جرائم الكمبيوتر والإنترنت .

ثمة تعريفات تستند الى موضوع الجريمة او احيانا الى انماط السلوك محل التجريم[1] ، وما من شك ان معيار موضوع الجريمة كاساس للتعريف يعد من اهم المعايير واكثرها قدرة على إيضاح طبيعة ومفهوم الجريمة محل التعريف ، على ان لا يغرق - كما يلاحظ على تعريف الأستاذ Rosenblatt - في وصف الأفعال ، اذ قد لا يحيط بها ، واذا سعى الى الاحاطة بها فانه سيغرق بالتفصيل الذي لا يستقيم وغرض وشكل التعريف ، هذا بالاضافة الى عدم وجود اتفاق حتى الآن، على الأفعال المنطوية تحت وصف جرائم الكمبيوتر. ورغم أن تعريف د. هدى قشقوش حاول تجاوز الوقوع في هذه المنزلقات، الا أنه جاء في الوقت ذاته عام يفقد التعريف ذاته مقدرته على بيان كنه الجريمة وتحديد الأفعال المنطوية تحتها.

اما التعريفات التي انطلقت من وسيلة ارتكاب الجريمة ، فان اصحابها ينطلقون من أن جريمة الكمبيوتر تتحقق باستخدام الكمبيوتر وسيلة لارتكاب الجريمة [2] ، وقد وجه لهذه التعريفات النقد ، من هذه الانتقادات ما يراه الأساتذة جون تابر John Taber و Michael Rostoker و Robert Rines من أن تعريف الجريمة يستدعي "الرجوع الى العمل الأساسي المكون لها وليس فحسب الى الوسائل المستخدمة

---

[1] ومنها تعريفها بانها "نشاط غير مشروع موجه لنسخ او تغيير او حذف او الوصول الى المعلومات المخزنة داخل الحاسب او التي تحول عن طريقه " (تعريف الاستاذ Rosenblatt ، مشار اليه لدى رستم ، السابق ، ص 31 .) وتعريفها بانها " كل سلوك غير مشروع او غير مسموح به فيما يتعلق بالمعالجة الالية للبيانات او نقل هذه البيانات " (تعريف الدكتوره هدى قشقوش ، جرائم الحاسب الالكتروني في التشريع المقارن، الطبعة الأولى دار النهضة العربية، القاهرة، 1992 ، ص 20) او هي " أي نمط من انماط الجرائم المعروف في قانون العقوبات طالما كان مرتبطا بتقنية المعلومات " (تعريف Artar Solarz) او هي " الجريمة الناجمة عن ادخال بيانات مزورة في الأنظمة واساءة استخدام المخرجات اضافة الى أفعال أخرى تشكل جرائم اكثر تعقيدا من الناحية التقنية مثل تعديل الكمبيوتر"(واحد من عدة تعريفات وضعها مكتب المحاسبة العامة للولايات المتحدة الامريكية GOA انظر :- www.goa.gov)

[2] من هذه التعريفات ، يعرفها الأستاذ جون فورستر (Tom forester, Essential proplems to Hig-Tech Society First MIT Pres edition, Cambridge, Massachusetts, 1989, P. 104) وكذلك الأستاذ Eslie D. Ball أنها " فعل اجرامي يستخدم الكمبيوتر في ارتكابه كأداة رئيسية" ويعرفها تايدمان Tiedemaun بانها "كل اشكال السلوك غير المشروع الذي يرتكب باستخدام الحاسوب" وكذلك يعرفها مكتب تقييم التقنية بالولايات المتحدة الأمريكية بأنها "الجريمة التي تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دورا رئيسا"

لتحقيقه"[1] ويعزز هذا النقد الأستاذ R. E. Anderson بقوله أنه "ليس لمجرد أن الحاسب قد استخدم في جريمة، ان نعتبرها من الجرائم المعلوماتية" .

جانب من الفقه والمؤسسات ذات العلاقة بهذا الموضوع ، وضعت عددا من التعريفات التي تقوم على اساس سمات شخصية لدى مرتكب الفعل ، وهي تحديدا سمة الدراية والمعرفة التقنية [2]. وفي معرض تقدير هذه التعريفات ، يمكننا القول ان شرط المعرفة التقنية ، شرط شخصي متصل بالفاعل ، غير أن هذه الجرائم كما سنرى في أمثلة عديدة يرتكب جزء كبير منها من قبل مجموعة تتوزع أدوارهم بين التخطيط والتنفيذ والتحريض والمساهمة ، وقد لا تتوفر لدى بعضهم المعرفة بتقنية المعلومات ثم ما هي حدود المعرفة التقنية ، وما هو معيار وجودها للقول بقيام الجريمة ؟؟؟ ان التطور الذي شهدته وسائل التقنية نفسها اظهر الاتجاه نحو تبسيط وسائل المعالجة وتبادل المعطيات ، وتحويل الاجهزة المعقدة فيما سبق الى اجهزة تكاملية سهلة الاستخدام حتى ممن لا يعرف شيئا في علوم الكمبيوتر ، ولم يعد مطلوبا العلم والمعرفة العميقين ليتمكن شخص من ارسال آلاف رسائل البريد الإلكتروني دفعة واحدة الى أحد المواقع لتعطيل عملها ، كما لم يعد صعبا ان يضمن أي شخص رسالة بريدية فيروسا التقطه كبرنامج عبر الإنترنت او من خلال صديق فيبثه للغير دون ان يكون عالما اصلا بشيء مما يتطلبه بناء مثل هذه البرامج الشريرة ، كما ان ما يرتكب الان باستخدام الهاتف الخلوي من انشطة اختراق واعتداء او ما يرتكب عليها من قبل اجهزة مماثلة يعكس عدم وجود ذات الاهمية للمعرفة التقنية او الدراية بالوسائل الفنية . اضف الى ذلك ان جانبا معتبرا من جرائم الكمبيوتر والإنترنت – يعتبر اخطرها في الحقيقة – تنسب المسؤولية فيه للشخص المعنوي، سيما وأن واحدة من المسائل الرئيسة فيما تثيره جرائم الكمبيوتر هي مسألة مسؤولية الشخص المعنوي ، شأنه شأن الشخص الطبيعي عن الأفعال المعتبرة جرائم كمبيوتر.

---

1 رستم ، المرجع السابق ، ص 31 .

2 من هذه التعريفات ، تعريف وزارة العدل الأمريكية في دراسة وضعها معهد ستانفورد للابحاث وتبنتها الوزارة في دليلها لعام 1979 ، حيث عرفت بانها " اية جريمة لفاعلها معرفة فنية بالحاسبات تمكنه من ارتكابها " . ومن هذه التعريفات أيضا تعريف David Thompson بانها " اية جريمة يكون متطلبا لاقترافها ان تتوافر لدى فاعلها معرفة بتقنية الحاسب " . وتعريف Stein Schjqlberg بانها " أي فعل غير مشروع تكون المعرفة بتقنية الكمبيوتر اساسية لارتكابه والتحقيق فيه وملاحقته قضائيا "

أمام قصور التعريفات المؤسسة على معيار واحد ، سواء القائمة على معيار قانوني موضوعي أو شخصي ، برز عدد من التعريفات ترتكز على أكثر من معيار لبيان ماهية جريمة الكمبيوتر ، من هذه التعريفات ، ما يقرره الأستاذ John Carrol ويتبناه الأستاذ Gion Green من أن جريمة الكمبيوتر هي "أي عمل ليس له في القانون أو أعراف قطاع الأعمال جزاء ، يضر بالأشخاص أو الأموال ، ويوجه ضد أو يستخدم التقنية المتقدمة (العالية) لنظم المعلومات"[1].

ويعتمد في التعريف كما نرى معايير عدة ، أولها، عدم وجود جزاء لمثل هذه الأفعال، وهو محل انتقاد بفعل توافر جزاءات خاصة لبعض هذه الجرائم لدى عدد ليس باليسير من التشريعات ، وثانيها، تحقيق الضرر للأشخاص أو الأموال . وثالثها توجه الفعل ضد أو استخدام التقنية المتقدمة لنظم المعلومات ، وهو معيار يعتمد موضوع الجريمة (تقنية نظم المعلومات) ووسيلة ارتكابها (أيضا تقنية نظم المعلومات) أساسا للتعريف. ولكن السؤال الذي يثور هنا، هل محل جريمة الكمبيوتر تقنية نظم المعلومات أم المعلومات ذاتها وفق دلالتها الواسعة والتي يعبر عنها على نحو أشمل وأدق بتعبير (معطيات الكمبيوتر) والتي تشمل البيانات المدخلة، البيانات المعالجة والمخزنة المعلومات المخزنة، المعلومات المخرجة، البرامج بأنواعها التطبيقية وبرامج التشغيل؟![2]

وقد عرف جريمة الكمبيوتر خبراء متخصصون من بلجيكا في معرض ردهم على استبيان منظمة التعاون الاقتصادي والتنمية OECD ، بانها " كل فعل او امتناع من شانه الاعتداء على الأمواج المادية او المعنوية يكون ناتجا بطريقة مباشرة او غير مباشرة عن تدخل التقنية المعلوماتية "[3].

والتعريف البلجيكي السالف، متبنى من قبل العديد من الفقهاء والدارسين بوصفه لديهم أفضل التعريفات لأن هذا التعريف واسع يتيح الاحاطة الشاملة قدر الامكان

[1] رستم ، ص 33 .

[2] كما يعرفها الأستاذ Sheldon. J. Hecht بأنها: "واقعة تتضمن تقنية الحاسب ومجني عليه يتكبد أو يمكن أن يتكبد خسارة وفاعل يحصل عن عمد أو يمكنه الحصول على مكسب" وقريب منه تعريف الفقيهDonn B. Parker في مؤلفه Fighting Computer Crime والذي يرى بأنها "أي فعل متعمد مرتبط بأي وجه، بالحاسبات، يتسبب في تكبد أو امكانية تكبد مجني عليه لخسارة أو حصول أو امكانية حصول مرتكبه على مكسب" ويستخدم للدلالة على الجريمة تعبير "إساءة استخدام الحاسوب".

ويلاحظ على هذين التعريفين ، خاصة الأول منهما ، أنه تعريف وصفي للجريمة لا تحديد لماهيتها عوضا عن أنه يعتمد من بين المعايير المتعددة معيار تحقق أو احتمال تحقق خسارة ، ولا يتسع هذا المعيار لحالات اختراق النظام والبقاء فيه دون أي مسلك آخر من شأنه تحقيق أو احتمال تحقيق خسارة .

[3] رستم – ص 33.

بظاهرة جرائم التقنية، ولأن التعريف المذكور يعبر عن الطابع التقني أو المميز الذي تنطوي تحته أبرز صورها، ولأنه أخيرا يتيح امكانية التعامل مع التطورات المستقبلية التقنية.

وبالرجوع للتعريف المتقدم نجد انه يشير الى امكان حصول جريمة الكمبيوتر بالامتناع ، وحسنا فعل في ذلك ، اذ اغفلت معظم التعريفات الاشارة الى شمول السلوك الاجرامي لجرائم الكمبيوتر صورة الامتناع رغم تحقق السلوك بهذه الطريقة في بعض صور هذه الجرائم كما سنرى . ومع اقرارنا بسعة التعريف المذكور وشموليته ، وبالجوانب الايجابية التي انطوى عليها، الا أننا نرى ان هذا التعريف اتسم بسعة خرجت به عن حدود الشمولية المطلوب وفقا لها احاطته بجرائم الكمبيوتر بالنظر لمحل الجريمة أو الحق المعتدى عليه ، هذه السعة التي أدخلت ضمن نطاقه جرائم لا تثير أية اشكالية في انطباق النصوص الجنائية التقليدية عليها ولا تمثل بذاتها ظاهرة جديدة، ونقصد تحديدا الجرائم التي تستهدف الكيانات المادية والاجهزة التقنية ، مع الاشارة الى ادراكنا في هذا المقام ان المقصود بالاموال المادية في التعريف انما هو استخدام الكمبيوتر للاستيلاء على اموال مادية ، لكن الاطلاقية التي تستفاد من التعبير تدخل في نطاق هذا المفهوم الأفعال التي تستهدف ذات ماديات الكمبيوتر او غيره من وسائل تقنية المعلومات.

ان الجرائم التي تطال ماديات الكمبيوتر ووسائل الاتصال ، شأنها شأن الجرائم المستقرة على مدى قرنين من التشريع الجنائي، محلها أموال مادية صيغت على أساس صفتها نظريات وقواعد ونصوص القانون الجنائي على عكس (معنويات) الكمبيوتر ووسائل تقنية المعلومات ، التي أفرزت أنشطة الاعتداء عليها تساؤلا عريضا – حسمت اجابته بالنفي - حول مدى انطباق نصوص القانون الجنائي التقليدية عليه.

ويعرف خبراء منظمة التعاون الاقتصادي والتنمية، جريمة الكمبيوتر بأنها :

"كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلق بالمعالجة الآلية للبيانات و/ أو نقلها"[1] وقد وضع هذا التعريف من قبل مجموعة الخبراء المشار اليهم للنقاش في اجتماع باريس الذي عقد عام 1983 ضمن حلقة (الاجرام المرتبط بتقنية المعلومات)، ويتبنى هذا التعريف الفقيه الالماني Ulrich Sieher ، ويعتمد هذا التعريف على معيارين : أولهما، (وصف السلوك). وثانيهما، اتصال السلوك بالمعالجة الآلية للبيانات أو نقلها[2].

ومن الفقه الفرنسي، يعرف الفقيه Masse جريمة الكمبيوتر (يستخدم اصطلاح الغش المعلوماتي) بأنها "الاعتداءات القانونية التي يمكن أن ترتكب بواسطة المعلوماتية بغرض تحقيق الربح"[3] وجرائم الكمبيوتر لدى هذا الفقيه جرائم ضد الأموال ، وكما نلاحظ يستخدم أساسا لهذا التعريف معيارين: أولهما الوسيلة مع تحفظنا على استخدام تعبير (بواسطة المعلوماتية). لأن المعلوماتية أو الأصوب، (تقنية المعلومات) هو المعالجة الآلية للبيانات، أي العملية لا وسائل تنفيذها.

أما المعيار الثاني ، المتمثل بتحقيق الربح ، المستمد من معيار محل الجريمة المتمثل بالمال لدى هذه الفقه، فقد أبرزنا النقد الموجه اليه، فالاعتداء في كثير من جرائم الكمبيوتر ينصب على المعلومات في ذاتها دون السعي لتحقيق الربح ودونما أن تكون المعلومات مجسدة لأموال او أصول، عوضا عن عدم صواب اعتبار المعلومات في ذاتها مالا ما لم يقر النظام القانوني هذا الحكم لها لدى سعيه لتوفير الحماية للمعلومات.

ويعرفها الفقهيين الفرنسيين Le stanc, Vivant بأنها : "مجموعة من الأفعال المرتبطة بالمعلوماتية والتي يمكن أن تكون جديرة بالعقاب".

---

[1] انظر موقع المنظمة على شبكة الانترنت www.oecd.org

[2] ومن ضمن التعريفات التي تعتمد أكثر من معيار، يعرف جانب من الفقه جريمة الكمبيوتر وفق معايير قانونية صرفه ، أولها تحديد محل الجريمة، وثانيها وسيلة ارتكابها وهو في كلا المعيارين (الكمبيوتر) لما يلعبه من دور الضحية ودور الوسيلة حسب الفعل المرتكب كما يرى هذا الجانب من الفقه. من هؤلاء الأستاذ Thomas. J. Smedinghoff في مؤلفه (المرشد القانوني لتطوير وحماية وتسويق البرمجيات). حيث يعرفها بأنها "أي ضرب من النشاط الموجه ضد أو المنطوي على استخدام نظام الحاسوب". وكما اسلفنا فتعبير (النشاط الموجه ضد) ينسحب على الكيانات المادية اضافة للمنطقية (المعطيات والبرامج). وكذلك تعريف الأستاذين Robert J. Lindquist و Jack Bologna " جريمة يستخدم الحاسوب كوسيلة mens أو أداة Instrument لارتكابها أو يمثل اغراء بذلك أو جريمة يكون الكمبيوتر نفسه ضحيتها" .

[3] انظر د. الدكتور سامي الشوا، الغش المعلوماتي كظاهرة اجرامية مستحدثة، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25-28 تشرين أول / أكتوبر 1993، ص 3.

وكما نرى فان هذا التعريف مستند من بين معيارية على احتمال جدارة الفعل بالعقاب ، وهو معيار غير منضبط البتة ولا يستقيم مع تعريف قانوني وان كان يصلح لتعريف في نطاق علوم الاجتماع أوغيرها.

-في تقدير اتجاهات التعريف والتعريف الملائم

لقد غرقت بعض التعريفات في التعامل مع جرائم الكمبيوتر كجرائم خاصة دون الاجابة مسبقا على موقع هذه الجرائم في نطاق القانون الجنائي ، بمعنى اذا كنا أمام ظاهرة اجرامية مستجدة تتميز من حيث موضوع الجريمة ووسيلة ارتكابها وسمات مرتكبيها وأنماط السلوك الاجرامي المجسدة للركن المادي لكل جريمة من هذه الجرائم ، أفلا يستدعي ذلك صياغة نظرية عامة لهذه الجرائم؟؟

هذه النظرية (العامة) ، أهي نظرية جنائية في نطاق القسم الخاص من قانون العقوبات ، لا تخلق اشكالات واسعة على الاقل - في تطبيق قواعد ونظريات القسم العام من قانون العقوبات ؟؟ أم ان هذه النظرية يجب أن تؤسس لقواعد وأحكام حديثة تطال قسمي القانون الخاص والعام؟![1].

ان طبيعة وأبعاد ظاهرة جرائم الكمبيوتر ، سيما في ظل تطور انماطها يوما بعد يوم مع تطور استخدام الشبكات وما اتاحته الإنترنت من فرص جديدة لارتكابها وخلقت انماطا مستجدة لها يشير الى تميزها في احكام لا توفرها النظريات القائمة ، تحديدا مسائل محل الاعتداء والسلوكيات المادية المتصلة بارتكاب الجرم ، وهذا ما أدى الى حسم الجدل الواسع حول مدى انطباق النصوص القائمة على هذه الجرائم لجهة وضع تشريعات ونصوص جديدة تكون قادرة على الاحاطة بمفردات ومتطلبات وخصوصية جرائم الكمبيوتر والإنترنت ، وهو بالتالي ما يحسم الجدل حول الحاجة الى نظرية عامة لجرائم الكمبيوتر توقف التوصيف الجزئي والمعالجات المبتسرة .

[1] يقول د. محمود نجيب حسني :

"ثمة نظريات للقسم الخاص لا صلة بينها وبين تطبيق القسم العام، ويكفي أن نشير الى نظريات العلانية في جرائم الاعتبار (الفعل الفاضح والسب)، والضرر في جرائم التزوير، والحيازة في السرقة والتدليس في النصب... لقد انتجت دراسة القسم الخاص نظريات لا تقل من حيث الخصوبة عن نظريات القسم العام...وعليه، يمكن القول بوجود نظريات عامة للقسم الخاص" الأستاذ الدكتور محمود نجيب حسني، شرح قانون العقوبات - القسم الخاص، بدون رقم الطبعة، دار النهضة العربية، القاهرة 1992. ص 4

ولا بد من التمييز في التعريف بين ظاهرة اجرام الحوسبة، أو كما يسميها قطاع واسع من الفقه المصري ظاهرة الجناح أو الانحراف المعلوماتي وبين جرائم الكمبيوتر والإنترنت . فتعريف الظاهرة مؤسس على مرتكزات عريضة وواسعة، هي في الغالب تعطي دلالة محل الظاهرة لكنها لا تنهض بايضاح هذا المحل على نحو عميق وشامل ووفق مرتكزات التعريف المطلوب في نطاق القانون الجنائي . أما تعريف الجريمة (عموما)، فكما ذكرنا إعلانية ، تتحقق فعاليته اذا ما أورد عناصرها وأثرها ، في حين أن التعريف لجريمة معينة يتطلب اظهار ركنها المادي المتمثل بالسلوك الاجرامي بشكل أساسي اضافة الى ما يتطلبه أحيانا من ايراد صورة الركن المعنوي أو العنصر المفترض أو غير ذلك.

وبالتالي فان الاعتداء على كيانات الاجهزة التقنية المادية (يتعدد وصفها ومهامها من الوجهة التقنية) يخرج من نطاق جرائم الكمبيوتر لترتد الى موقعها الطبيعي وهو الجرائم التقليدية ، باعتبار هذه الماديات مجسدة لمال منقول مادي تنهض به قواعد ومبادئ ونصوص القانون الجنائي واذا كان من وجوب الحديث عن الاعتداءات على الكيانات المادية في نطاق ظاهرة جرائم الكمبيوتر والإنترنت ، فانه متعلق فقط بقيمتها الاستراتيجية كمخازن للمعلومات وأدوات لمعالجتها وتبادلها ، مما يستدعي نقاش تطوير آليات حمايتها ، خاصة من أنشطة الإرهاب والتخريب المعادية للتقنية (كموقف سياسي او ايديولوجي) ولكن في نطاق النصوص التقليدية لا في نطاق ظاهرة جرائم الكمبيوتر المستجدة ، مع التنبه الى ان أفعال الاتلاف والتدمير المرتكبة في نطاق جرائم الكمبيوتر والإنترنت ، هي الموجهة للنظم والمعطيات وليس لماديات الاجهزة .

اما عن دور الكمبيوتر في الجريمة ، فانه متعدد في الحقيقة ، فهو اما ان يكون الهدف المباشر للاعتداء ، او هو وسيلة الاعتداء لتحقيق نتيجة جرمية لا تتصل مباشرة بالمعطيات وانما بما تمثله او تجسده ، او هو بيئة ومخزن للجريمة ، ويجب أن لا يوقعنا أي من هذه الادوار في أي خلط بشان محل الجريمة أو وسيلة ارتكابها فان محل جريمة دائما هو المعطيات (أما بذاتها أو بما تمثله) ووسيلة ارتكاب جريمة

الكمبيوتر والإنترنت الكمبيوتر او أي من الاجهزة التكاملية التقنية (أي التي تدمج بين تقنيات الاتصال والحوسبة) وعلى أن يراعى ان دلالة نظام الكمبيوتر تشمل نظم تقنية المعلومات المجسدة في الكمبيوتر المحقق لتوأمة الحوسبة والاتصال في عصر التقنية الشاملة المتقاربة.

واذا كانت تعريفات الجريمة عموما تقوم على أساسين : عناصر الجريمة و السلوك ووصفه، والنص القانوني على تجريم السلوك وايقاع العقوبة، فان الجديد في مجال جرائم الكمبيوتر هو اضافة عنصر ثالث يبرز محل الاعتداء في هذه الظاهرة الاجرامية المستحدثة ، متمثلا بمعطيات الحاسوب. فقانون العقوبات ينطوي على نصوص تحرم الاعتداء على الأشخاص ، الأموال ، الثقة العامة ... الخ لكن المستجد ، هو الكيانات المعنوية ذات القيمة المالية أو القيمة المعنوية البحتة أو كلاهما، ولولا هذه الطبيعة المستجدة في الأساس لما كنا أمام ظاهرة مستجدة برمتها، ولكان المستجد هو دخول الكمبيوتر عالم الاجرام ، تماما كما هو الشأن في الجرائم المنظمة، فهي في الحقيقة جرائم تقليدية المستجد فيها عنصر التنظيم الذي ينتج مخاطر هائلة واتساع نطاق المساهمة الجنائية وانصهار الارادات الجرمية في ارادة واحدة هي ارادة المنظمة الاجرامية المعنية .

وعلينا التاكيد هنا على ان جرائم الكمبيوتر ليست مجرد جرائم تقليدية بثوب جديد او بوسيلة جدية فهذا قد ينطبق على بعض صور الجرائم التي يكون الكمبيوتر فيها وسيلة لارتكاب الجريمة ، وليس صحيحا ما قاله الكثير من الاعلاميين الغربيين في المراحل الأولى لظاهرة الكمبيوتر انها ليست اكثر من (نبيذ قديم في زجاجة جديدة) . انها بحق ، جرائم جديدة في محتواها ونطاقها ومخاطرها ، ووسائلها ومشكلاتها ، وفي الغالب في طبائع وسمات مرتكبيها .

على ضوء ما تقدم من استخلاصات واستنتاجات فاننا في معرض تحديد ماهية هذه الجرائم والوقوف على تعريفها ، نخلص للنتائج التالية : -

1 - ان الاعتداء على الكيانات المادية للكمبيوتر وأجهزة الاتصال يخرج عن نطاق جرائم الكمبيوتر لان هذه الكيانات محل صالح لتطبيق نصوص التجريم التقليدية

المنظمة لجرائم السرقة والاحتيال واساءة الامانة والتدمير والاتلاف وغير ذلك باعتبار ان هذه السلوكيات تقع على مال مادي منقول ، والأجهزة تنتسب الى هذا النطاق من الوصف كمحل للجريمة .

2 - ان مفهوم جريمة الكمبيوتر مر بتطور تاريخي تبعا لتطور التقنية واستخداماتها ، ففي المرحلة الأولى من شيوع استخدام الكمبيوتر في الستينات ومن ثم السبعينات ، ظهرت اول معالجات لما يسمى جرائم الكمبيوتر - وكان ذلك في الستينات - واقتصرت المعالجة على مقالات ومواد صحفية تناقش التلاعب بالبيانات المخزنة وتدمير أنظمة الكمبيوتر والتجسس المعلوماتي والاستخدام غير المشروع للبيانات المخزنة في نظم الكمبيوتر ، وترافقت هذه النقاشات مع التساؤل حول ما إذا كانت هذه الجرائم مجرد شيء عابر أم ظاهرة جرمية مستجدة ، بل ثار الجدل حول ما إذا كانت جرائم بالمعنى القانوني أم مجرد سلوكيات غير اخلاقية في بيئة او مهنة الحوسبة ، وبقي التعامل معها اقرب الى النطاق الاخلاقي منه الى النطاق القانوني ، ومع تزايد استخدام الحواسيب الشخصية في منتصف السبعينات ظهرت عدد من الدراسات المسحية والقانونية التي اهتمت بجرائم الكمبيوتر وعالجت عددا من قضايا الجرائم الفعلية ، وبدأ الحديث عنها بوصفها ظاهرة جرمية لا مجرد سلوكيات مرفوضة . وفي الثمانينات طفا على السطح مفهوم جديد لجرائم الكمبيوتر ارتبط بعمليات اقتحام نظم الكمبيوتر عن بعد وانشطة نشر وزراعة الفايروسات الإلكترونية ، التي تقوم بعمليات تدميرية للملفات او البرامج ، وشاع اصطلاح (الهاكرز) المعبر عن مقتحمي النظم ، لكن الحديث عن الدوافع لارتكاب هذه الأفعال ظل في غالب الاحيان محصورا بالحديث عن رغبة المخترقين في تجاوز إجراءات أمن المعلومات وفي اظهار تفوقهم التقني، وانحصر الحديث عن مرتكبي الأفعال هذه بالحديث عن صغار السن من المتفوقين الراغبين بالتحدي والمغامرة ، والى مدى نشأت معه قواعد سلوكية لهيئات ومنظمات الهاكرز طالبوا معها بوقف تشويه حقيقتهم واصرارهم على انهم يؤدون خدمة في التوعية لأهمية معايير أمن النظم والمعلومات ، لكن الحقيقة ان مغامري الامس اصبحوا عتاة

اجرام فيما بعد ، الى حد إعادة النظر في تحديد سمات مرتكبي الجرائم وطوائفهم وظهر المجرم المعلوماتي المتفوق المدفوع بأغراض جرمية خطرة ، القادر على ارتكاب أفعال تستهدف الاستيلاء على المال او تستهدف التجسس او الاستيلاء على البيانات السرية الاقتصادية والاجتماعية والسياسية والعسكرية . وشهدت التسعينات تناميا هائلا في حقل الجرائم التقنية وتغيرا في نطاقها ومفهومها ، وكان ذلك بفعل ما احدثته شبكة الإنترنت من تسهيل لعمليات دخول الأنظمة واقتحام شبكات المعلومات ، فظهرت انماط جديدة كانشطة انكار الخدمة التي تقوم على فكرة تعطيل نظام تقني ومنعه من القيام بعمله المعتاد ، واكثر ما مورست ضد مواقع الإنترنت التسويقية الناشطة والهامة التي يعني انقطاعها عن الخدمة لساعات خسائر مالية بالملايين . ونشطت جرائم نشر الفايروسات عبر مواقع الإنترنت لما تسهله من انتقالها الى ملايين المستخدمين في ذات الوقت ، وظهرت انشطة الرسائل والمواد الكتابية المنشورة على الإنترنت او المرسلة عبر البريد الإلكتروني المنطوية على اثارة الاحقاد او المساس بكرامة واعتبار الأشخاص او المستهدفة الترويج لمواد او أفعال غير قانونية وغير مشروعة (جرائم المحتوى الضار).

3 - ان محل جريمة الكمبيوتر هو دائما المعطيات اما بذاتها او بما تمثله هذه المعطيات التي قد تكون مخزنة داخل النظام او على أحد وسائط التخزين او تكون في طور النقل والتبادل ضمن وسائل الاتصال المندمجة مع نظام الحوسبة .

4 - ان كل جرم يمس مصلحة يقدر الشارع اهمية التدخل لحمايتها ، والمصلحة محل الحماية في ميدان جرائم الكمبيوتر هي الحق في المعلومات (كعنصر معنوي ذي قيمة اقتصادية عالية) ويشمل ذلك الحق في الوصول الى المعلومات وانسيابها وتدفقها وتبادلها وتنظيم استخدامها كل ذلك على نحو مشروع ودون مساس بحقوق الآخرين في المعلومات .

5 - ان تعريف الجريمة عموما يتأسس على بيان عناصرها المناط بالقانون تحديدها ، اذ من دون نص القانون على النموذج القانوني للجريمة لا يتحقق امكان المساءلة عنها (سندا الى قاعدة الشرعية الجنائية التي توجب عدم جواز العقاب عند

انتفاء النص ، وسندا الى ان القياس محظور في ميدان النصوص التجريمية الموضوعية) ، وهو ما يستوجب التمييز بين الظاهرة الجرمية والجريمة . ولذلك فان ظاهرة جرائم الكمبيوتر تعرف وفق التحديد المتقدم بانها (الأفعال غير المشروعة المرتبطة بنظم الحواسيب)[1] اما تعريف جريمة الكمبيوتر فانها (سلوك غير مشروع معاقب عليه قانونا صادر عن ارادة جرمية محله معطيات الكمبيوتر) فالسلوك يشمل الفعل الإيجابي والامتناع عن الفعل ، وهذا السلوك غير مشروع باعتبار المشروعية تنفي عن الفعل الصفة الجرمية ، ومعاقب عليه قانونا لان اسباغ الصفة الاجرامية لا يتحقق في ميدان القانون الجنائي الا بارادة المشرع ومن خلال النص على ذلك حتى لو كان السلوك مخالفا للاخلاق . ومحل جريمة الكمبيوتر هو دائما معطيات الكمبيوتر بدلالتها الواسعة (بيانات مدخلة ، بيانات ومعلومات معالجة ومخزنة البرامج بانواعها ، المعلومات المستخرجة ، والمتبادلة بين النظم) واما الكمبيوتر فهو النظام التقني بمفهومه الشامل المزاوج بين تقنيات الحوسبة والاتصال ، بما في ذلك شبكات المعلومات.

-تحديد عام للسمات والخصائص في ضوء التعريف والمحل

اذن ، جرائم الكمبيوتر في نطاق الظاهرة الاجرامية المستحدثة – التي بدو انها لم تعد كذلك بالنظر ان اول حالة موثقة لجريمة الكترونية تعود لعام 1959 وبالنظر لنحو 36 عاما من التعايش الدولي مع صور مختلفة ومتغايرة من هذ الجرائم جرائم تنصب على معطيات الحاسوب (بيانات ومعلومات وبرامج) وتطال الحق في المعلومات، ويستخدم لاقترافها وسائل تقنية تقتضي استخدام الحاسوب بوصفه نظاما حقق التزاوج بين تقنيات الحوسبة والاتصالات.

[1] طبعا بالمفهوم الشامل لنظام الكمبيوتر المدمج فيه تقنيات الاتصال وشبكات المعلومات كالانترنت

- جرائم الكمبيوتر والانترنت طائفة من الجرائم التي تتسم بسمات مخصوصة عن غيرها من الجرائم ، فهي تستهدف معنويات وليست ماديات محسوسة ، وتثير في هذا النطاق مشكلات الاعتراف بحماية المال المعلوماتي ان جاز التعبير
- كما انها تتسم بالخطورة البالغة نظرا لاغراضها المتعددة . ونظرا لحجم الخسائر الناجم عنها قياسا بالجرائم التقليدية . ونظرا لارتكابها من بين فئات متعددة تجعل من التنبؤ بالمشتبه بهم امرا صعبا . ونظرا لانها بذاتها تنطوي على سلوكيات غير مالوفة ، وبما اتاحته من تسهيل ارتكاب الجرائم الاخرى تمثل ايجاد وسائل تجعل ملاحقة الجرائم التقليدية امرا صعبا متى ما ارتكبت باستخدام الكمبيوتر.
- وتحقيق وتحري جرائم الكمبيوتر والانترنت والمقاضاة في نطاقها تنطوي على مشكلات وتحديات ادارية وقانونية تتصل ابتداء بمعيقات ومتطلبات عمليات ملاحقة الجناة ، فان تحققت مكنة الملاحقة اصبحت الادانة صعبة لسهولة اتلاف الادلة من قبل الجناة او لصعوبة الوصول الى الادلة او لغياب الاعتراف القانوني بطبيعة الادلة المتعلقة بهذه الجرائم . ونظرا لانها جرائم لا تحدها حدود وتعد من الجرائم العابرة للحدود ، فتثير لذلك تحديات ومعيقات في حقل الاختصاص القضائي والقانون الواجب التطبيق ومتطلبات التحقيق والملاحقة والضبط والتفتيش . .

ان جرائم الكمبيوتر قد ترتكب عن طريق حاسب آلي في دولة ما، في حين يتحقق الفعل الاجرامي في دولة أخرى"[1] فجرائم الكمبيوتر والانترنت ، لا تحدها حدود ولا تعترف ابتداء – في هذه المرحلة من تطورها بسبب شبكات المعلومات – بعنصر المكان او حدود الجغرافيا ، وتتميز بالتباعد الجغرافي بين الفاعل والمجني عليه ومن الوجهة التقنية ، بين الحاسوب أداة الجريمة ، وبين المعطيات أو البيانات محل

[1] الأستاذ (Ulrich Seiber) - جرائم الحاسب الآلي والجرائم الأخرى المرتبطة بالتقنيات الحديثة لوسائل الاتصال، ترجمة الدكتور سامي الشوا، ورقة عمل مقدمة للمؤتمر السادس للجمعية المصرية للقانون الجنائي، 25-28، تشرين أول/أكتوبر 1993 - والورقة المذكورة بذاتها من أوراق التحضير للمؤتمر الخامس عشر للجمعية الدولية لقانون العقوبات - (البرازيل 4 - 9 أيلول 1994).ص8.

الجريمة في نظام الحاسوب المستهدفة بالاعتداء ، هذا التباعد قد يكون ضمن دائرة الحدود الوطنية للدولة، لكنه ، وبفعل سيادة تقنيات شبكات النظم والمعلومات ، امتد خارج هذه الحدود - دون تغيير في الاحتياجات التقنية - ليطال دولة أخرى يتواجد فيها نظام الحاسوب المخزنة فيه المعطيات محل الاعتداء.

والحقيقة أن مسألة التباعد الجغرافي بين الفعل وتحقق النتيجة من أكثر المسائل التي تثير اشكالات في مجال جرائم الحاسوب وبشكل خاص الاجراءات الجنائية ووالاختصاص والقانون الواجب التطبيق. وهذا بدوره عامل رئيس في نماء دعوات تظافر الجهود الدولية لمكافحة هذه الجرائم، ولعل هذه السمة تذكرنا بارهاصات جرائم المخدرات والاتجار بالرقيق وغيرها من الجرائم التي وقف تباين الدول واختلاف مستويات الحماية الجنائية فيها حائلا دون نجاعة أساليب مكافحتها،فلم يكن من بد غير الدخول في سلسلة اتفاقيات ومعاهدات دولية لمكافحة هذه الجرائم ، وذات الامر يقال الان بشان انشطة غسل الاموال ، وهي في ذات الوقت الأسباب ذاتها التي تجعل موضوع جرائم الارهاب والجرائم المنظمة والجرائم الاقتصادية المواضيع الرئيسة على اجندة اهتمام المتمع الدولي [1].

ولمواجهة مثل هذه الجريمة (جريمة الحاسوب) العابرة للحدود مواجهة فعالة، يجب تجريم صورها في القانون الوطني للمعاقبة عليها، وان يكون هناك تعاون وتضامن دولي لمواجهة مشاكلها من حيث مكان وقوعها واختصاص المحاكم بها وجمع المعلومات والتحريات عنها والتنسيق بين الدول في المعاقبة عليها وتحديد صورها وقواعد التسليم فيها وايجاد الحلول لمشكلاتها الاساسية وابرزها: - ." [2]

1 - غياب مفهوم عام متفق عليه بين الدول -حتى الآن - حول نماذج النشاط المكون للجريمة المتعلقة بالكمبيوتر والانترنت .

2 - غياب الاتفاق حول التعريف القانوني للنشاط الاجرامي المتعلق بهذا النوع من الاجرام.

---

[1] انظر ، الأستاذ الدكتور محمد محي الدين عوض. مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، ورقة عمل مقدمة الى المؤتمر السادس للجمعية المصرية للقانون الجنائي،القاهرة 25-28 تشرين أول 1993. ص 6.

[2] السابق ، ص 6.

3 - نقص الخبرة لدى الشرطة وجهات الادعاء والقضاء في هذا المجال لتمحيص عناصر الجريمة ان وجدت وجمع المعلومات والأدلة عنها للادانة فيها.

4 -عدم كفاءة وملاءمة السلطات التي ينص عليها القانون بالنسبة للتحري واختراق نظم الكمبيوتر، لأنها عادة متعلقة بالضبط والتحري بالنسبة لوقائع مادية هي الجرائم التقليدية وغير متوائمة مع غير (الماديات) كاختراق المعلومات المبرمجة وتغييرها في الكمبيوتر.

5 -عدم التناسب بين قوانين الإجراءات الجنائية للدول المختلفة فيما يتعلق بالتحري في الجرائم المتعلقة بالحاسوب.

6 - السمة الغالبة للكثير من جرائم الكمبيوتر هي أنها – كما اوضحنا اعلاه - من النوع العابر للحدود Transnational وبالتالي تثير من المشاكل ما تثيره أمثال تلك الجرائم كجرائم الاتجار بالمخدرات والاتجار غير المشروع في الأسلحة والاتجار في الرقيق الأبيض والجرائم الاقتصادية والمالية وجرائم التلوث البيئي.

7 - عدم وجود معاهدات للتسليم أو للمعاونة الثنائية أو الجماعية بين الدول تسمح بالتعاون الدولي أو عدم كفايتها ان كانت موجودة لمواجهة المتطلبات الخاصة لجرائم الكمبيوتر ودينامية التحريات فيها وكفالة السرعة بها". ويمثل مشروع الاتفاقية الاوروبية لجرائم الكمبيوتر في الوقت الحاضر المشروع الاكثر نضجا لموجهة جرائم الكمبيوتر بل وواحدا من اهم ادوات التعاون الدولي في هذا الحقل .

وعوضا عن هذه المشكلات، فاننا نرى أن من أبرز المشاكل التي تواجه سياسات مكافحة جرائم الحاسوب لا على الصعيد الدولي بل وفي نطاق التشريعات الوطنية عدم التعامل معها كوحدة واحدة في اطار الحماية الجنائية للمعلومات. وقد عالجنا هذه المسألة في الكتاب الاول من هذه الموسوعة - اذ أن التعامل على الصعيد الدولي وكذلك على صعيد التشريع الوطني بشأن توفير الحماية الجنائية للمعلومات قد تم -كما يذكر الفقيه Utrich seiber - من خلال السعي لتشييد الحماية

الجنائية لكل من الحياة الخاصة، الأموال (المعلومات المجسدة للمال على ما نرى) والحقوق الذهنية ازاء اجرام تقنية المعلومات، كل على حده.[1]

2 - الاتجاهات المتعددة لتصنيف الجرائم الالكترونية وموقع جرائم الاعتداء على الخصوصية وحقوق الملكية الفكرية ضمنها

2 -1 تصنيف الجرائم تبعا لنوع المعطيات ومحل الجريمة .

هذا التصنيف هو الذي ترافق مع موجات التشريع في ميدان قانون تقنية المعلومات[2]، وهو التصنيف الذي يعكس ايضا التطور التاريخي لظاهرة جرائم الكمبيوتر والانترنت ، ونجده التصنيف السائد في مختلف مؤلفات الفقيه الالماني (الريش سيبر – Ulrich Zebar) والمؤلفات المتاثرة به ولهذا نجد أن جرائم الكمبيوتر بالاستناد الى هذا المعيار يمكن تقسيمها ضمن الطوائف التالية : -

أولا : الجرائم الماسة بقيمة معطيات الحاسوب، وتشمل هذه الطائفة فئتين، أولهما الجرائم الواقعة على ذات المعطيات، كجرائم الاتلاف والتشويه للبيانات والمعلومات وبرامج الحاسوب بما في ذلك استخدام وسيلة (الفيروسات) التقنية. وثانيهما الجرائم الواقعة على ما تمثله المعطيات آليا، من أموال أو أصول، كجرائم غش الحاسوب التي تستهدف الحصول على المال أو جرائم الاتجار بالمعطيات ، وجرائم التحوير والتلاعب في المعطيات المخزنة داخل نظم الحاسوب واستخدامها (تزوير المستندات المعالجة آليا واستخدامها).

ثانيا :الجرائم الماسة بالمعطيات الشخصية او البيانات المتصلة بالحياة الخاصة وتشمل جرائم الاعتداء على المعطيات السرية أو المحمية وجرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة وهو ما يعرف بموضوع (الخصوصية) .

---

[1] يقول الفقيه (Seiber): وقد ابان التحليل للقوانين المختلفة، ان الحماية الجنائية للمعلومات في كل دولة، بحاجة ماسة لوضع نظرية عامة لها، ومرد ذلك، أنه في غالبية الحالات، فان الحماية الجنائية لكل من الحياة الخاصة والأموال، والحقوق الذهنية ازاء اجرام تقنية المعلومات قد تم مناقشتها كل على حده - المرجع السابق – ورقة العمل – ص 4.

[2] انظر حول التطور التاريخي لجرائم الكمبيوتر تفصيلا (ضمن سياق التطور التاريخي لقانون الكمبيوتر وفروعه) مؤلفنا – قانون الكمبيوتر السابق الاشارة اليه .

ثالثا :الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسوب ونظمه (جرائم قرصنة البرمجيات) التي تشمل نسخ وتقليد البرامج واعادة انتاجها وصنعها دون ترخيص واستغلالها ماديا والاعتداء على العلامة التجارية وبراءة الاختراع.

وبامعان النظر في هذه الطوائف، نجد أن الحدود بينها ليست قاطعة ومانعة فالتداخل حاصل ومتحقق، اذ أن الاعتداء على معطيات الحاسوب بالنظر لقيمتها الذاتية أو ما تمثله، هو في ذات الوقت اعتداء على أمن المعطيات، لكن الغرض المباشر المحرك للاعتداء انصب على قيمتها أو ما تمثله. والاعتداء على حقوق الملكية الفكرية لبرامج الحاسوب، هو اعتداء على الحقوق المالية واعتداء على الحقوق الأدبية (الاعتبار الأدبي) لكنها تتميز عن الطوائف الأخرى بأن محلها هو البرامج فقط وجرائمها تستهدف الاستخدام غير المحق أو التملك غير المشروع لهذه البرامج.

هذا من جهة، ومن جهة أخرى، نجد أن الحماية الجنائية للمعلومات في نطاق القانون المقارن وفي اطار الجهود الدولية لحماية معطيات الحاسوب واستخدامه اعتمدت على نحو غالب، التقسيم المتقدم فظهرت حماية حقوق الملكية الأدبية للبرامج ، وحماية البيانات الشخصية المتصلة بالحياة الخاصة ، وحماية المعطيات بالنظر لقيمتها أو ما تمثله والذي عرف بحماية (الأموال)، كل في ميدان وموقع مستقل. وهو في الحقيقة تمييز - ليس مطلقا - بين حماية قيمة المعطيات وأمنها، وحقوق الملكية الفكرية. ولا بد لنا من الاشارة، ان حماية أمن المعطيات (الطائفة الثانية) انحصر في حماية البيانات الشخصية المتصلة بالحياة الخاصة، أما حماية البيانات والمعلومات السرية والمحمية فقد تم تناوله في نطاق جرائم الطائفة الثالثة الماسة بقيمة المعطيات بالنظر الى أن الباعث الرئيسي للاعتداء والغرض من معرفة أو افشاء هذه المعلومات غالبا ما كان الحصول على المال مما يعد من الاعتداءات التي تندرج تحت نطاق الجرائم الماسة بقيمة المعطيات التي تتطلب توفير الحماية الجنائية للحقوق المتصلة بالذمة المالية التي تستهدفها هذه الجرائم.

2 -2 تصنيف الجرائم تبعا لدور الكمبيوتر في الجريمة .

اشرنا في غير موضع من مؤلفاتنا التي تناولت جرائم الكمبيوتر الى دور الكمبيوتر في الجريمة، وخلصنا انه قد يكون هدف الاعتداء ، بمعنى ان يستهدف الفعل المعطيات المعالجة او المخزنة او المتبادلة بواسطة الكمبيوتر والشبكات ، وهذا ما يعبر عنه بالمفهوم الضيق (لجرائم الكمبيوتر) وقد يكون الكمبيوتر وسيلة ارتكاب جريمة اخرى في اطار مفهوم (الجرائم المرتبطة بالكمبيوتر)، وقد يكون الكمبيوتر اخيرا بيئة الجريمة او وسطها او مخزنا للمادة الجرمية ، وفي هذا النطاق هناك مفهومان يجري الخلط بينهما يعبران عن هذا الدور : - الاول جرائم التخزين ، ويقصد بها تخزين المواد الجرمية او المستخدمة في ارتكاب الجريمة او الناشئة عنها ، والثاني ، جرائم المحتوى او ما يعبر عنه بالمحتوى غير المشروع او غير القانوني والاصطلاح الاخير استخدم في ضوء تطور اشكال الجريمة مع استخدام الانترنت ، واصبح المحتوى غير القانوني يرمز الى جرائم المقامرة ونشر المواد الاباحية والغسيل الالكتروني للاموال وغيرها باعتبار ان مواقع الانترنت تتصل بشكل رئيس بهذه الانشطة .

والحقيقة ان المفهومين يتصلان بدور الكمبيوتر والشبكات كبيئة لارتكاب الجريمة وفي نفس الوقت كوسيلة لارتكابها . وهذا التقسيم شائع بجزء منه (وهو تقسيم الجرائم الى جرائم هدف ووسيلة) لدى الفقه المصري والفرنسي[1] ، وتبعا له تنقسم جرائم الكمبيوتر الى جرائم تستهدف نظام المعلوماتية نفسه كالاستيلاء على المعلومات واتلافها ، وجرائم ترتكب بواسطة نظام الكمبيوتر نفسه كجرائم احتيال الكمبيوتر .

اما تقسيمها كجرائم هدف ووسيلة ومحتوى فانه الاتجاه العالمي الجديد في ضوء تطور التدابير التشريعية في اوروبا تحديدا ، وافضل ما يعكس هذا التقسيم الاتفاقية الاوروبية لجرائم الكمبيوتر والانترنت لعام 2001 (اتفاقية بودابست 2001) ، ذلك

---

[1] انظر د. احمد حسام طه تمام ، المرجع السابق ، ود. سعيد عبد اللطيف حسن ، المرجع السابق ، ود . محمد سامي الشوا ، الكتاب ، المرجع السابق ، ود. هدى قشوش، المرجع السابق ، ود جميل عبد الباقي الصغير، القانون الجنائي والتكنولوجيا الحديثة، الكتاب الأول، الجرائم الناشئة عن استخدام الحاسب الآلي، الطبعة الأولى، منشورات دار النهضة العربية، القاهرة، 1992، وبالفرنسية Pieere Catala, ***Ebauche Duune Theorie Juridique de ,information*** ,1983, Andre Lucas, ***Protiction of information Bases***, Kuwait First Conference, Ministry of Justice, 15-17 Feb.1999, Kuwait. وغيرها

ان العمل منذ مطلع عام 2000 يتجه الى وضع اطار عام لتصنيف جرائم الكمبيوتر والانترنت وعلى الاقل وضع قائمة الحد الادنى محل التعاون الدولي في حقل مكافحة هذه الجرائم ، وهو جهد تقوده دول اوروبا لكن وبنفس الوقت بتدخل ومساهمة من قبل استراليا وكندا وامريكا ، وضمن هذا المفهوم نجد الاتفاقية المشار اليها تقسم جرائم الكمبيوتر والانترنت الى الطوائف التالية – مع ملاحظة انها تخرج من بينها طائفة جرائم الخصوصية لوجود اتفاقية اوروبية مستقلة تعالج حماية البيانات الاسمية من مخاطر المعالجة الالية للبيانات – اتفاقية 1981 .

لقد أوجدت اتفاقية بودابست 2001 تقسيما جديدا نسبيا ، فقد تضمن اربع طوائف رئيسة لجرائم الكمبيوتر والانترنت .

الاولى : – الجرائم التي تستهدف عناصر السرية والسلامة وديمومة توفر المعطيات والنظم وتضم : –

- الدخول غير قانوني (غير المصرح به) .
- الاعتراض غير القانوني .
- تدمير المعطيات .
- اعتراض النظم .
- اساءة استخدام الاجهزة .

الثانية : الجرائم المرتبطة بالكمبيوتر وتضم : –

- التزوير المرتبط بالكمبيوتر .
- الاحتيال المرتبط بالكمبيوتر .

الثالثة : الجرائم المرتبطة بالمحتوى وتضم طائفة واحدة وفق هذه الاتفاقية وهي الجرائم المتعلقة بالافعال الاباحية واللاأخلاقية .

الرابعة : الجرائم المرتبطة بالاخلال بحق المؤلف والحقوق المجاورة – قرصنة البرمجيات .

2 -3 تصنيف الجرائم تبعا لمساسها بالاشخاص والاموال .

نجد هذا التصنيف شائعا في الدراسات والابحاث الامريكية – مع فروق بينها من حيث مشتملات التقسيم ومدى انضباطيته ، كما نجده المعيار المعتمد لتقسيم جرائم الكمبيوتر والانترنت في مشروعات القوانين النموذجية التي وضعت من جهات بحثية بقصد محاولة ايجاد الانسجام بين قوانين الولايات المتحدة المتصلة بهذا الموضوع ، وابرز تقسيم في هذا الصدد ذلك الذي تضمنه مشروع القانون النموذجي لجرائم الكمبيوتر والانترنت الموضوع عام 1998 من قبل فريق بحثي اكاديمي والمسمى Model State Computer Crimes Code ، وفي نطاقه تم تقسيم جرائم الكمبيوتر والانترنت الى ، الجرائم الواقعة على الاشخاص ، والجرائم الواقعة على الاموال عدا السرقة ، وجرائم السرقة والاحتيال ، وجرائم التزوير ، وجرائم المقامرة والجرائم ضد الاداب – عدا الجرائم الجنسية ، والجرائم ضد المصالح الحكومية ويلاحظ ان التقسيم يقوم على فكرة الغرض النهائي او المحل النهائي الذي يستهدفه الاعتداء ، لكنه ليس تقسيما منضبطا ولا هو تقسيم محدد الاطر فالجرائم التي تستهدف الاموال تضم من حيث مفهومها السرقة والاحتيال فقط اما الجرائم التي تستهدف التزوير فتمس الثقة والاعتبار ، والجرائم الواقعة ضد الاداب قد تتصل بالشخص وقد تتصل بالنظام والاخلاق العامة ، وعلى العموم فانه وتبعا لهذا التقسيم – الوارد ضمن مشروع القانون النموذجي الامريكي [1] – تصنف جرائم الكمبيوتر على النحو التالي: -

[1] في عرضنا التفصيلي لهذا القانون وتقسيماته اشرنا ازاء كل صورة جريمة الى قانون الولاية ورقم المادة التي تضمنت تلك الصورة في الحالات التي كانت فيها مشمولة بالنص مشيرين ان غرض هذا القانون النموذجي وضع مسطرة للتشريع الملائم لضم كل صور جرائم الكمبيوتر بتسمياتها المختلفة ، ونجدها فرصة للتنبه الى ان ثمة معضلة اصطلاحات خلقها عدم دقة الاستخدام الاعلامي لصور هذه الجرائم وارتباطها كثيرا بالتقنيات المستخدمة مع ان اكثر من تقنية قد تتعلق بالصورة الواحدة ، في هذا السياق انظر مسرد المصطلحات التعريبي لمصطلحات قانون الكمبيوتر المنشور ضمن اجزاء موسعتنا (القانون والتقنية العالية) الموزع ضمن كتب هذه الموسعة تبعا لموضوع كل كتاب .

2 -3 -1 طائفة الجرائم التي تستهدف الاشخاص : -

وتضم طائفتين رئيستين هما : -

1 - الجرائم غير الجنسية التي تستهدف الاشخاص Non-Sexual Crimes Against Persons وتشمل القتل بالكمبيوتر Computer Murder ، والتسبب بالوفاة جرائم الاهمال المرتبط بالكمبيوتر Negligent Computer Homicide والتحريض على الانتحار Soliciting or Encouraging Suicide ، والتحريض القصدي للقتل عبر الانترنت Intentional Internet Homicide Solicitation والتحرش والمضايقة عبر وسائل الاتصال المؤتمتة Harassment via Computerized Communication والتهديد عبر وسائل الاتصال المؤتمتة Intimidation via Computerized Communication والاحداث المتعمد للضرر العاطفي او التسبب بضرر عاطفي عبر وسائل التقنية Malicious Infliction of Emotional Distress utilizing Computer Communication و Reckless Infliction of Emotional Distress utilizing Computer Communication والملاحقة عبر الوسائل التقنية Stalking وانشطة اخلاس النظر او الاطلاع على البيانات الشخصية Online Voyeurism and Online Voyeurism Disclosure وقنابل البريد الالكتروني E-mail Bombing وانشطة ضخ البريد الالكتروني غير المطلوب او غير المرغوب به Spamming utilizing Computerized Communication وبث المعلومات المضللة او الزائفة Transmission of False Statements والانتهاك الشخصي لحرمة كمبيوتر (الدخول غير المصرح به) Personal trespass by computer

2 - طائفة الجرائم الجنسية Sexual Crimes : - وتشمل حض وتحريض القاصرين على انشطة جنسية غير مشروعة Soliciting a Minor with a Computer for Unlawful Sexual Purposes وافساد القاصرين باشطة جنسية عبر الوسائل الالكترونية Corrupting a Minor with the use of a

واغواء او محاولة اغواء Computer for Unlawful Sexual Purposes.
Luring or Attempted Luring القاصرين لارتكاب انشطة جنسية غير مشروعة
وتلقي of a Minor by Computer for Unlawful Sexual Purposes
او نشر المعلومات عن القاصرين عبر الكمبيوتر من اجل انشطة جنسية غير مشروعة
Receiving or Disseminating Information about a Minor by
والتحرش الجنسي Computer for Unlawful Sexual Purposes
Sexually Harassing a minor بالقاصرين عبر الكمبيوتر والوسائل التقنية
ونشر وتسهيل by use of a Computer for Unlawful Sexual Purposes
نشر واستضافة المواد الفاحشة عبر الانترنت بوجه عام وللقاصرين تحديدا
Posting Or و Posting Obscene Material On The Internet.
Trafficking In و Receiving Obscene Material On The Internet
Sending Obscene Material و Obscene Material On The Internet
ونشر الفحش والمساس بالحياء (هتك To Minors Over The Internet
Indecent Exposure On The Internet العرض بالنظر) عبر الانترنت
Depicting Minors Engaged وتصوير او اظهار القاصرين ضمن انشطة جنسية
In Sexually Explicit Conduct--Pandering Obscenity Involving A
Minor واستخدام الانترنت لترويج الدعارة بصورة قسرية او للاغواء او لنشر المواد
Using الفاحشة التي تستهدف استغلال عوامل الضعف والانحراف لدى المستخدم
Using the Internet for و the Internet for Compelling Prostitution
Using the Internet و Using the Internet for Soliciting و Pimping
و الحصول على الصور والهويات بطريقة غير for Promoting Prostitution
Unauthorized Appropriation of مشروعة لاستغلالها في انشطة جنسية
Identity, Image, or Likeness for Unlawful Sexual Purposes

وبامعان النظر في هذه الاوصاف نجد انها تجتمع جميعا تحت صورة واحدة هي استغلال الانترنت والكمبيوتر لترويج الدعارة او اثارة الفحش واستغلال الاطفال والقصر في انشطة جنسية غير مشروعة.

2 -3-2 طائفة جرائم الاموال – عدا السرقة - او الملكية المتضمنة انشطة الاختراق والاتلاف (Property Damage (Other than Theft and Crimes Involving Intrusions

وتشمل انشطة اقتحام او الدخول او التوصل غير المصرح به مع نظام الكمبيوتر او الشبكة اما مجردا او لجهة ارتكاب فعل اخر ضد البيانات والبرامج والمخرجات Computer Trespass و Aggravated Computer Trespass و Disorderly Persons Offense وتخريب المعطيات والنظم والممتلكات ضمن مفهوم تخريب الكمبيوتر Computer Vandalism وايذاء الكمبيوتر Computer Mischief واغتصاب الملكية Extortion وخلق البرمجيات الخبيثة والضارة Creation of Harmful Programs و نقلها عبر النظم والشبكات Transmission of Harmful Programs و واستخدام اسم النطاق او العلامة التجارية او اسم الغير دون ترخيص Cybersquatting وادخال معطيات خاطئة او مزورة الى نظام كمبيوتر Introducing False Information Into a Computer or Computer System و لالتعديل غير المصرح به لاجهزة ومعدات الكمبيوتر Unlawful Modification of Computer Equipment or Supplies والاتلاف غير المصرح به لنظم الكميوتر (مهام نظم الكمبيوتر الادائية) Unlawful Modification of Computer Equipment or Supplies وانشطة انكار الخدمة او تعطيل او اعتراض عمل النظام او الخدمات Unlawful Denial, Interruption, or Degradation of Access to Computer و Unlawful Denial, Interruption, or Degradation of Access to Computer Services وانشطة الاعتداء على الخصوصية Invasion of Privacy (وهذه تخرج عن مفهوم الجرائم التي تستهدف الاموال لكنها تتصل بجرائم الاختراق) وافشاء كلمة سر الغير Disclosure of Another's Password والحيازة غير المشروعة للمعلومات Unauthorized Possession of Computer Information و واساءة استخدام المعلومات

و نقل معلومات خاطئة Misuse of Computer Information . Transmission of False Data

2 -3 -3 جرائم الاحتيال والسرقة Fraud and Theft Crimes

وتشمل جرائم الاحتيال بالتلاعب بالمعطيات والنظم Fraud by Computer Manipulation واستخدام الكمبيوتر للحصول على او استخدام البطاقات المالية للغير دون ترخيص Using a Computer to Fraudulently Obtain and Use Credit Card Information او تدميرها Damaging or Enhancing Another's Credit Rating والاختلاس عبر الكمبيوتر او بواسطته Computer Embezzlement وسرقة معلومات الكمبيوتر Computer Information Theft وقرصنة البرامج Software Piracy وسرقة خدمات الكمبيوتر (وقت الكمبيوتر) Theft of Computer Services وسرقة ادوات التعريف والهوية عبر انتحال هذه الصفات او المعلومات داخل الكمبيوتر Computer Impersonation .

2 -3 -4 جرائم التزوير Forgery

وتشمل تزوير البريد الالكتروني Electronic Mail Forgery (E-Mail Forgery) وتزوير الوثائق والسجلات Document/Record Forgery و تزوير الهوية Identity Forgery .

2 -3 -5 جرائم المقامرة والجرائم الاخرى ضد الاخلاق والاداب Gambling and Other Offenses Against Morality

وتشمل تملك وادارة مشروع مقامرة على الانترنت Owning and Operating an Internet Gambling business وتسهيل ادارة مشاريع القمار على الانترنت Facilitating the operation of an Internet gambling business وتشجيع مشروع مقامرة عبر الانترنت Patronizing an Internet Gambling Business واستخدام الانترنت لترويج الكحول ومواد الادمان للقصر Using the Internet to provide liquor to minors و Using the Internet to

Using the Internet to provide و provide cigarettes to minors . prescription drugs

Crimes Against the جرائم الكمبيوتر ضد الحكومة 6- 3- 2 ،Government

وتشمل هذه الطائفة كافة جرائم تعطيل الاعمال الحكومية وتنفيذ القانون Obstructing enforcement of law or other government function والاخفاق في الابلاغ عن جرائم الكمبيوتر Failure to report a cybercrime والحصول على معلومات سرية Obtaining confidential government information والاخبار الخاطيء عن جرائم الكمبيوتر False Reports of Cybercrimes والعبث بالادلة القضائية او التاثير فيها Tampering with evidenc و Tampering with a Computer Source Document وتهديد السلامة العامة Endangering Public Safety وبث البيانات من مصادر مجهولة Anonymity كما تشمل الارهاب الالكتروني Cyber-Terrorism والانشطة الثارية الالكترونية او انشطة تطبيق القانون بالذات Cyber-Vigilantism.

2 -4 تصنيف الجرائم كجرائم الكمبيوتر وجرائم الانترنت .

في سياق الحديث عن الاصطلاحات المستخدمة للتعبير عن ظاهرة جرائم الكمبيوتر والانترنت ، وتحديدا الوقوف امام تاثر الاصطلاحات بالمرحلة التاريخية التي نشات فيها انماط هذه الجرائم تبعا للتطور في حقل التقنية ، فان من الطبيعي ان يكون ثمة مفهوم لجرائم ترتكب على الكمبيوتر وبواسطته قبل ان يشيع استخدام شبكات المعلومات وتحديدا الانترنت ، ومن الطبيعي ان تخلق الانترنت انماطا جرمية مستجدة او ان تؤثر بالالية التي ترتكب فيها جرائم الكمبيوتر ذاتها بعد ان تحقق تشبيك الكمبيوترات معا في نطاق شبكات محلية واقليمية وعالمية ، او على الاقل تطرح انماط فرعية من الصور القائمة تختص بالانترنت ذاتها ، ومن هنا جاء هذا التقسيم ، وسنجد انه وان كان مبررا من حيث المنطلق فانه غير صحيح في الوقت

الحاضر بسبب سيادة مفهوم نظام الكمبيوتر المتكامل الذي لا تتوفر حدود وفواصل في نطاقه بين وسائل الحوسبة (الكمبيوتر) ووسائل الاتصال (الشبكات) .

وفي نطاق هذا المعيار يجري التمييز بين الافعال التي تستهدف المعلومات في نطاق نظام الكمبيوتر ذاته – خلال مراحل المعالجة والتخزين والاسترجاع – وبين الانشطة التي تستهدف الشبكات ذاتها او المعلومات المنقولة عبرها ، وطبعا الانشطة التي تستهدف مواقع الانترنت وخوادمها من نظم الكمبيوتر الكبيرة والعملاقة او تستهدف تطبيقات واستخدامات وحلول الانترنت وما نشا في بيئتها من اعمال الكترونية وخدمات الكترونية .

وفي اطار هذه الرؤيا ، نجد البعض يحصر انشطة جرائم الانترنت بتلك المتعلقة بالاعتداء على المواقع وتعطيلها او تشويهها او تعطيل تقديم الخدمة (انشطة انكار الخدمة وانشطة تعديل وتحوير محتوى المواقع او المساس بعنصري ديمومة التوفر والتكاملية او سلامة المحتوى) وكذلك انشطة المحتوى الضار ، كترويج المواد الاباحية والمقامرة ، وانشطة اثارة الاحقاد والتحرش والازعاج (تحديدا عبر الانترنت وانشطة المطارة والتحرش والابتزاز ، ومختلف صور الانشطة التي تستخدم البريد الالكتروني والمراسلات الالكترونية وغرف الحوار ، وانشطة الاستيلاء على كلمات سر المستخدمين والهوية ووسائل التعريف ، وانشطة الاعتداء على الخصوصية عبر جمع المعلومات من خلال الانترنت ، وانشطة احتيال الانترنت كاحتيال المزادات وعدم التسليم الفعلي للمنتجات والخدمات ، وانشطة نشر الفايروسات والبرامج الخبيثة عبر الانترنت ، وانشطة الاعتداء على الملكية الفكرية التي تشمل الاستيلاء على المواد والمصنفات المحمية واساءة استخدام اسماء النطاقات او الاستيلاء عليها او استخدامها خلافا لحماية العلامة التجارية ، وانشطة الاعتداء على محتوى المواقع والتصميم ، وانشطة الروابط غير المشروعة ، وانشطة الاطر غير المشروعة (وهي انشطة يقوم من خلالها احد المواقع باجراء مدخل لربط مواقع اخرى او وضعها ضمن نطاق الاطار الخارجي لموقعه هو) ، وغيرها من الجرائم التي يجمعها مفهوم (جرائم الملكية الفكرية عبر الانترنت) .

اما جرائم الكمبيوتر فانها وفق هذا التقسيم تعاد الى الانشطة التي تستهدف المعلومات والبرامج المخزنة داخل نظم الكمبيوتر وتحديدا انشطة التزوير واحتيال الكمبيوتر وسرقة المعطيات وسرقة وقت الحاسوب واعتراض المعطيات خلال النقل (مع انه مفهوم يتصل بالشبكات اكثر من نظم الكمبيوتر) طبعا اضافة للتدخل غير المصرح به والذي يتوزع ضمن هذا التقسيم بين دخول غير مصرح به لنظام الكمبيوتر ودخول غير مصرح به للشبكات فيتبع لمفهوم جرائم الانترنت .

ولو وقفنا على هذا التقسيم فاننا بالضرورة ودون عناء سنجده تقسيما غير دقيق وغير منضبط على الاطلاق ، بل ومخالف للمفاهيم التقنية وللمرحلة التي وصل اليها تطور وسائل تقنية المعلومات وعمليات التكامل والدمج بين وسائل الحوسبة والاتصال ، ففي هذه المرحلة ، ثمة مفهوم عام لنظام الكمبيوتر يستوعب كافة مكوناته المادية والمعنوية المتصلة بعمليات الادخال والمعالجة والتخزين والتبادل ، مما يجعل الشبكات وارتباط الكمبيوتر بالانترنت جزء من فكرة تكاملية النظام .

هذا من جهة ، ومن جهة اخرى ، فان انشطة الانترنت تتطلب اجهزة كمبيوتر تقارف بواسطتها ، وهي تستهدف ايضا معلومات مخزنة او معالجة ضمن اجهزة كمبيوتر ايضا هي الخوادم التي تستضيف مواقع الانترنت او تديرها ، واذا اردنا ان نتحكم في فصل وسائل تقنية المعلومات ، فان هذا لن يتحقق لان الشبكات ذاتها عبارة عن حلول وبرمجيات وبروتوكولات مدمجة في نظام الحوسبة ذاته الا اذا اردنا ان نحصر فكرة الشبكات بالاسلاك واجهزة التوجيه (الموجهات) ، وهذا يخرجنا من نطاق جرائم الكمبيوتر والانترنت الى جرائم الاتصالات التي تستهدف ماديات الشبكة ، مشيرين هنا ان الموجهات التي قد يراها البعض تجهيزات تتصل بالشبكة ما هي في الحقيقة الا برامج تتحكم بحركة تبادل المعطيات عبر الشبكة .

ويعدو المعيار غير صحيح البتة اذا ما عمدنا الى تحليل كل نمط من انماط الجرائم المتقدمة في ضوء هذا المعيار ، فعلى سبيل المثال ، تعد جريمة الدخول غير المصرح به لنظام الكمبيوتر وفق هذا المعيار جريمة كمبيوتر اما الدخول غير المصرح به الى موقع انترنت فانها جريمة انترنت ، مع ان الحقيقة التقنية ان الدخول

في الحالتين هو دخول الى نظام الكمبيوتر عبر الشبكة. ولو اخذنا مثلا جريمة انكار الخدمة وتعطيل عمل النظام ، فسواء وجهت الى نظام كمبيوتر ام موقع انترنت فهي تستهدف نظام الكمبيوتر الذي هو في الحالة الاولى كمبيوتر مغلق وفي الثانية كمبيوتر يدير موقع انترنت .

هذه هي اهم نظريات التصنيف ، ولاننا اوردنا ملاحظاتنا حول كل منها ، فاننا نكتفي في معرض تقديرها بالقول ان اكثر التقسيمات انضباطية – لكنه ليس تقسيما مطلقا في انضباطيته – هو معيار تصنيف هذه الجرائم تبعا لدور الكمبيوتر في الجريمة .

3 - في مفهوم ومحددات قائمة الحد الادني من صور الجرائم الالكترونية [1].

3 -1 جريمة التوصل او الدخول غير المصرح به

تعد أنشطة الدخول او التوصل غير المصرح به او غير المخول به Unauthorized Access ، الانشطة الجرمية الاكثر انتشارا most windespread بين جرائم الكمبيوتر والانترنت ، ويقوم التوصل غير المصرح به بالاساس على الدخول الى نظام الحاسوب او شبكة المعلومات ، عادة من خلال استخدام وسيلة اتصال عن بعد (كالموديم modem) او من خلال التوصل عبر نقاط الاتصال والموجهات الموجودة على الشبكة للدخول الى نظام كمبيوتر معين بغرض التوصل مع البيانات او البرامج المخزنة في النظام ، ويتطلب هذا النشاط غالبا تجاوز او كسر اجراءات الحماية التقنية للنظام system security ، كتجاوز كلمة السر pssword واجراءات التعريف والجدران النارية وغيرها او التوصل لنقطة ضعف في نظام حماية البرامج والنفاذ منها .

ومعظم الذين يرتكبون هذه الانشطة بآلياتها التقنية المتعددة تكون انشطتهم مجردة عن اغراض لاحقة ، ولا يكون هدفهم – في الغالب – الاضرار بالبيانات

[1] مجرد عرض موجز للصور ومحدداتها وللوقوف على تفاصيل هذه الور وغيرها وحالات عملية بشانها والموقف التفصيلي للقوانين المقارنة بشانها راجع مؤلفنا – جرائم الكمبيوتر والانترنت – المرجع السابق ، الفصل الرابع وما بعده .

والملفات او تدميرها destroying data or files ، وفي الغالب يسعى مقترفو هذه الانشطة الى الاطلاع على المعلومات المحمية . غير ان حماية المعلومات من اخطار هذه الانشطة ، واحتمال تطور هذه الانشطة من مجرد هدف الاطلاع الى اهداف اكثر خطورة كالتلاعب بالمعطيات او اتلافها او ارتكاب غير ذلك من جرائم الحاسوب او استخدام الدخول لارتكاب جرائم اخرى بواسطة الكمبيوتر ، دفعت غالبية دول العالم الى تجريم هذه الانشطة كما هو الشأن في قوانين كل الدول الاوروبية وامريكا واليابان.

ومن الوجهة التقنية ، يمثل فعل التوصل غير المصرح به مع نظام الحاسوب الفعل الاول من بين انشطة جرائم الكمبيوتر والانترنت ، قد ينتهي النشاط به وقد يمتد النشاط الى ابعد من مجرد التوصل ، وهذه الحقيقة التقنية تثير الجدل حول ما اذا كان التوصل غير المصرح به بذاته فعلا جرميا ، فيجرم لذلك مجرد الدخول الى النظام حتى لو لم يكن ثمة فعل آخر لاحق لها السلوك، ام انه مجرد فعل تحضيري لجرم لاحق – ان ارتكب – غير مجرم بذاته . ثم اذا اعقب التوصل اتيان فعل آخر؟! فهل نكون امام تعدد في الجرائم ، ام ان التوصل يمثل حالة الشروع في الجريمة التي هدف الى ارتكابها بفعل التوصل ؟! ثم ما هي الأفعال المكونة للركن المادي لهذه الجريمة عند النص عليها استقلالا عن اي فعل لاحق ؟! وما هي الوسائل التقنية لاتيان هذه الأفعال ؟!

-موقف القوانين المقارنة بشأن جريمة التوصل غير المصرح به مع نظام الكمبيوتر

ان القوانين المقارنة التي وضعت لمواجهة جرائم الحاسوب ، جرمت في غالبيتها جريمة التوصل غير المصرح به مع نظام الحاسوب . لكنها تتفاوت في تحديد المراد بهذه الجريمة ، ففي القانون الفرنسي (1988 المعدل لعام 1994) يجرم المشرع مجرد التوصل مع نظام الحاسوب او البقاء فيه ، وكذلك ينهج ذات القانون البريطاني (1990) مع تباين في نطاق الأفعال المكونة للجريمة بين القانونيين ، في حين نجد القانون الامريكي (1984 والتشريعات اللاحقة عليه) يقرن فعل الاتصال بدون

تصريح مع تحقيق نتائج محددة ، كالحصول على المعلومات او استخدام النظام او اتلاف المعطيات . وتتردد بقية القوانين محل الدراسة بين هذه الاتجاهات ، فنجد قوانين معظم الولايات الامريكية سلكت مسلك القانون البريطاني في تجريم مجرد التوصل مع نظام الحاسوب ، فنص قانون كاليفورنيا لعام 1985 على انه يعتبر مرتكبا لجنحة كل من دخل عمدا الى منظومة أو شبكة حواسيب او الى برنامج او بيانات عالما بحظر ذلك من قبل مالكها او مستأجرها ، ولعل مسلك القوانين الخاصة بالولايات الامريكية يستند الى منهج مشروع القانون الفدرالي لحماية نظم الحاسوب لسنة 1984 ، الذي جرم في المادة الثانية الاتصال عمدا بغير تصريح لحاسوب او بنظام حاسوب او بشبكة تتضمن حاسوبا . ، ونجد مثلا ، القانون السويسري ينهج منهج القانون الامريكي (قانون غش واساءة استخدام الحاسوب لسنة 1984) وعلى هدي مسلك القانونين الفرنسي والانجليزي سلكت معظم القوانين الاوروبية .

3 -2 جريمة الاستيلاء على المعطيات ؟؟

يعرف الاستاذ محمود نجيب حسني السرقة ، بانها " اعتداء على ملكية منقول وحيازته بنية تملكه " وعرفها قانون العقوبات الأردني في المادة (1/399) بانها " اخذ مال الغير المنقول دون رضاه " وحدد المراد باخذ المال بانه " ازالة تصرف المالك فيه برفعه من مكانه ونقله ، واذا كان متصلا بغير منقول فبفصله عنه فصلا تاما ونقله " (م 2/399) وقرر ان لفظه مال تشمل القوى المحرزة (م 3/399) ، وهذا المفهوم لجريمة السرقة يمثل – في غالبية عناصره – ذات المفهوم المقرر في مختلف القوانين العربية [1].

وجريمة السرقة ، اعتداء على حق الملكية ، ولهذا فان الملكية هي المحل الرئيسي للاعتداء ، وهي كذلك اعتداء على الحيازة من اجل استطاعة الاعتداء على الملكية . واما موضوع جريمة السرقة ، فهو (المال المنقول) وفق القانون الأردني واللبناني

---

[1] انظر في تفصيل ذلك د. محمود نجيب حسني ، القسم الخاص ، المرجع السابق ، ص 88 وما بعدها . وكذلك مؤلفه الأستاذ الدكتور محمود نجيب حسني - جرائم الاعتداء على الأموال في قانون العقوبات اللبناني - دراسة مقارنة، الطبعة الأولى، دار النهضة العربية للطباعة والنشر، بيروت، 1984. ود. عبد العظيم وزير ، المرجع السابق ، وكذلك الأستاذ الدكتور كامل السعيد، شرح قانون العقوبات الأردني، الجرائم الواقعة على الأموال الطبعة الثانية، دار الثقافة للنشر والتوزيع، عمان، 1991.

(م 635) والكويتي (م 217) والقطري (م21) والسوري (م 621) والمغربي (م 505) وقانون ابو ظبي (م 78) . وهو (المنقول) وفق القانون المصري ، (والشئ) وفق العديد من قوانين العقوبات المقارنة كالفرنسي (م 379) والبلجيكي والهولندي (م 310) والتونسي (م 258) والبحريني (م 231) (والشئ المنقول) وفق القانون الالماني (م 242) والايطالي (م 624) والسويسري (م 137) . و (الشئ المادي) وفق القانون النمساوي (م 127) . وجامع هذه الاوصاف لتحديد محل السرقة ان تتوفر الصفة المادية في المحل وان يكون مالا (كل شئ يصلح محلا لحق عيني) لان الحيازة التي تنالها السرقة بالاعتداء ، يراد بها الحيازة المادية ، المتمثلة بسيطرة الحائز على الشئ ومباشرة سلطاته المادية عليه ، وان يكون محل السرقة مملوك للغير اذ لا تقوم السرقة اذا كان المال مملوكا للمتهم أو كان لغير المالك . وان يكون منقولا ، وهو ما يتم نقله من مكان إلى مكان دون تلف ، وقد الحق بالمنقول العقارات بالتخصيص والعقارات بالاتصال ، وعلة تطلب ان يكون محل السرقة منقولا هو ان فعل الاخذ أو الاختلاس (كما يسمى في القانون المصري) يتطلب تغيير موضع الشئ كوسيلة لاخراجه من حيازة المجني عليه .

وقد توسعت النظم القانونية في دلالة تعبير المال أو الشئ المادي ، اما عبر الاجتهاد القضائي أو بنصوص صريحة في قوانين العقوبات ، فادخلت في نطاقه القوى المحرزة كالطاقة الكهربائية ، اما استنادا إلى اعتبار الكهرباء ذات كيان مادي ملموس وتصلح محلا للملكية والحيازة ، أو بالاستناد إلى قيمة الكهرباء وان كانت مجرد حالة للمادة . وليس المقام تحليل الاتجاهات في مسألة صلاحية القوى المحرزة لتكون محلا لجريمة السرقة، ونكتفي بالقول ان الموقف من تجريم سرقة الكهرباء في بداياته يشابه إلى حد بعيد الجدل الحاد الذي دار حول صلاحية معطيات الحاسوب وكذلك صلاحية المعلومات عموما للسرقة ، هذا الجدل الذي لم يحسم الا باقرار نصوص خاصة تجرم الاعتداء على القوى المحرزة .[1]

[1] انظر المراجع المشار اليها في الهامش السابق .

وتتطلب جريمة السرقة – عموما – توافر الركن المادي المتمثل بفعل الاخذ دون رضى المالك (القانون الأردني) أو الاختلاس وفقا للقانون المصري ، والنتيجة الجرمية المتمثلة لخروج الشئ محل السرقة من حيازة المجني عليه إلى حيازة الجاني ، وعلاقة السببية التي تربط الفعل بالنتيجة . وحيث ان الاعتداء في السلوك الاجرامي ينصب على حيازة الغير ، فان عنصر الاخذ أو الاختلاس يتعين تحديده بالاستناد إلى نظرية الحيازة [1] ، ويعرف تبعا لذلك بانه " اخراج الشئ من حيازة المجني عليه دون رضاه وادخاله في حيازة اخرى " [2]

واما الركن المعنوي في جريمة السرقة ، فيتخذ صورة القصد الجنائي ، ولا يكفي الجريمة توفر القصد العام متمثلا بعنصري العلم والارادة ، وانما يتطلب ركن السرقة المعنوي قصدا خاصا ، يتمثل بنية تملك المال موضوع السرقة ، وتقوم هذه النية على عنصرين : سلبي ، يتمثل بارادة حرمان المالك من سلطاته على الشئ ومظهره العزم على عدم رد الشئ . وعنصر ايجابي ، قوامه ، ارداة المتهم ان يحل محل المالك في سلطاته على الشئ ، وبالتالي فان نية التملك كما يقول د. محمود نجيب حسني " لا تتجه إلى الملكية كحق ، ولكن تتجه إليها كمركز واقعي وفحوى اقتصادي ، أي مجموعة من السلطات والمزايا الفعلية " [3].

هذه هي المعالم الرئيسة لجريمة السرقة في القانون الجنائي التقليدي ، وليس المقام التوسع في تناول احكامها ، غير أننا في معرض بيان الاتجاهات حول امكان انطباق نصوص جريمة السرقة على جريمة الاستيلاء على المعطيات سنتعرض حسبما تقتضي الدراسة إلى جوانب اخرى من احكام هذه الجريمة.

في ضوء هذا التحديد هل ينطبق نص الرقة التقليدي على الاستيلاء على المعطيات ؟؟

---

[1] الدكتور نور الدين هنداوي، الحماية الجنائية للحيازة، الطبعة الأولى، دار النهضة العربية، القاهرة، 1993.

[2] انظر د. حسني ، و د. السعيد ، المرجعين السابقين المشار اليهما في الهامش 182.

[3] د. حسني ، المرجع السابق ، ص 866 .

يرصد الفقه [1] ثلاث صور يتحقق فيها الاستيلاء على معطيات الحاسوب: -

اولها : - الالتقاط الذهني للبيانات بالنظر أو الاستماع ، ويتم هذا الالتقاط " بالاختزان أو الحفظ الواعي أو العرضي للمعلومات اثر مطالعتها بالبصر ان كانت قد ظهرت على شاشة الحاسوب في شكل مرئي ، أو بعد وصولها إلى الاذن ان تمثلت في صورة صوتية صادرة على الاجهزة .

وثانيها : - النسخ غير المشروع للبيانات المخزنة الكترونيا ، اما عن طريق التعامل المباشر مع نظام الحاسوب ، المخزنة فيه البيانات على هيئة نبضات كهربائية في الدارات المدمجة ، أو على وسائط التخزين الرئيسة أو الثانوية (hard & flopy disk) ، واما عن طريق التوصل غير المرخص به مع نظام الحاسوب ، عبر الاتصال عن بعد كما عرضنا فيما تقدم .

وثالثها : - اعتراض معطيات الحاسوب خلال نقلها والتقاطها بواسطة احدى الطرق التي عرضنا لها سابقا . اما صورة الاستيلاء على الدعامات المادية المتضمنة للبيانات ، فقد اكدنا في غير مقام ، انها لا تثير مشاكل في تطبيق النصوص الجنائية التقليدية المشيدة على حماية الاموال المادية .

والسؤال الذي يثور في هذا المقام ، هل يعتبر الاستيلاء المتحقق في هذه الاساليب أو ما تماثلها أو ينشأ من اساليب تقنية للاستيلاء على معطيات الحاسوب – في ظل تطور الوسائل التقنية واساليب وتكتيك الجناة - مما يدخل في نطاق السلوك الاجرامي المكون لجريمة السرقة التقليدية ؟

لما كانت نصوص جريمة السرقة التقليدية – كما اسلفنا – تتطلب ان ينصب سلوك الجاني على شئ ذي طبيعة مادية ، فان اولى مشكلات تطبيق نصوص السرقة على الاستيلاء على المعطيات ، عدم توافر الطبيعة المادية لها.

اما المشكلة الثانية ، فهي مدى اعتبار المعطيات مالا بذاتها ، وهو من قوام عناصر موضوع أو محل جريمة السرقة .

[1] انظر في هذا الصدد د. رستم ، المرجع السابق .

والمشكلة الثالثة مدى قابلية المعطيات للحيازة باعتبار ان السلوك الاجرامي (الفعل) في اطار الركن المادي للجريمة يقوم بالاستيلاء على الحيازة .

تعد مسألة تحديد طبيعة المعطيات ، حجر الاساس في تقدير الموقف من قابلية انطباق النصوص التقليدية . لا على جريمة السرقة فحسب ، بل وعلى طائفة معتبرة من جرائم الحاسوب . وما اثير بشانها من خلاف حاد ومتعارض ، اشبه ما يكون بالخلاف الذي اثير حول مدى شمول نصوص السرقة لانشطة الاستيلاء على القوى المحرزة كالكهرباء وخطوط الهاتف . وكذلك يقع هذا الخلاف في نطاق الجدل الدائر حول امكان وقوع السرقة على المعلومات عموما ، مجردة من دعاماتها المادية كالورق أو المستندات أو غير ذلك .

ويكاد يكون متفقا عليه ، في الفقه واتجاهات القضاء ، ان الاستيلاء على المعطيات من خلال التقاطها الذهني ، بالنظر واستراق السمع ، لا يقوم به فعل الاخذ أو الاختلاس في جريمة السرقة التقليدية

ان الاتجاهات الفقهية ، واحكام القضاء بعد اخذ ورد اتفقت على عدم امكان انطباق نصوص السرقة على الاستيلاء على معطيات الحاسوب أو المعلومات عموما لغياب الصفة المادية ولعدم اعتبارها من قبيل الاموال التي يقع عليها السلوك الاجرامي في جريمة السرقة . وانعكس هذا الموقف على اتجاه التشريعات المقارنة التي ذهبت الى النص صراحة على جرم الاستيلاء على المعلومات (سرقتها) بالرغم من سعة بعض نصوص السرقة التقليدية في النظم المقارنة ، يقدم الدليل المعزز على صحة حجج هذا الاتجاه القائل بعدم امكان تطبيق نصوص السرقة التقليدية على جريمة الاستيلاء على المعلومات .

ان نصوص السرقة في قوانين العقوبات العربية القائمة لا يمكن ان تطبق على جرائم الاستيلاء على معطيات الكمبيوتر ، باية مرحلة كانت عليها هذه المعطيات من نظام المعالجة او النقل ونستند في هذا الراي الى ما يلي : -

1 -تخلف الطبيعة المادية لمعطيات الحاسوب ، وكذا المعلومات الذي لا ينفيه العديد من مؤيدي بسط النصوص التقليدية على صور الاعتداء عليها .

2 - واستنادا الى ان المعلومات ليست مالا في ذاتها ، مع ادراكنا الكلي لان المعلومات اصبحت المحدد الاستراتيجي لراس المال بل واهم عناصر الذمة المالية – برابنا – في العصر الرقمي الذي نعيش .

3 -ان المعلومات غير قابلة للحيازة المادية وفقا للفهم القانوني المستقر في اطار نظرية الحماية الجنائية للحيازة التي تاسست عليها نصوص السرقة التقليدية .

4 -وبالاستناد إلى ان اقوى ركائز الاتجاه الفقهي والقضائي المؤيد لبسط نصوص السرقة التقليدية يتمثل بالوصف الذي يحدده النموذج القانوني لمحل الجريمة بـ (الشئ) غير منعوتا بصفة دالة على تحديده ، خلافا للوصف السائد في تشريعات الدول العربية (مال منقول ، او منقول او منقول مادي او نحوها)) وبالاستناد إلى ان العديد من هذه الاراء ،قد خلط بين مرتكزات الحماية الجنائية للملكية ، ومرتكزات حماية الملكية الفكرية وحقوق المؤلف .

5 - ان المستقر في فقه القانون الجنائي ، ان محل جريمة السرقة هو المال المنقول ذو الطبيعة المادية المملوك للغير ، ولذلك فان ابعد مدى قد وصله التوسع في مد ، بل ومط النصوص الجنائية في هذا المجال ، طال في القليل من قضاء الدول ، تجريم سرقة القوى المحرزة ولم تسوغه الغالبية الا عبر النص التشريعي صراحة .

6 -ان الجهد المبذول في تطويع النصوص التقليدية ، لا يتفق مع تسارع وتيرة التطور في ميدان السلوك الاجرامي خاصة في عصر التقنية .

7 -ان من اهم المبادئ المستقرة في القانون الجنائي ، مبدا الشرعية الذي يحظر العقاب على اي سلوك دون ان يكون مجرما صراحة بموجب النص القانوني . ومبدأ وحظر القياس في النصوص الجنائية الموضوعية الذي يمنع القياس من اصله فلا يقبل معه قياس سرقة الماديات على الاستيلاء على المعنويات ، لا لانغلاق العقل عن مقتضيات التطور – كما يرى البعض - ولكن لاتصال هذه المبادئ باعلى قيم الانفتاح ، وهما كفالة العدالة وحماية حقوق الإنسان والشرعية الدستورية .

8 -وانطلاقا من تميز ركائز الحماية الجنائية للمعلومات عموما ومعطيات الحاسوب عن حماية الاموال المادية ، التي تستدعي اقامة التوازن بين الحق في تدفق

وانسياب المعلومات ومنع احتكارها ، وبين اليات حماية الاعتداء عليها ، والقيود القانونية المنظمة لهذا الحق الآخذ في النماء كحق متميز من حقوق الإنسان المؤسسة على التضامن الاجتماعي .

9 -واستنادا إلى ان التمييز بين صور الاستيلاء التقنية على المعلومات ، لا يأخذ بعين الاعتبار ما يحمله المستقبل من تطورها وتبدلها ، كما انه يجافي المنطق الذي يرفض تغيير الاحكام بشان ذات الموضوع (محل الجريمة) بتغير الوسيلة التقنية .

10 -واخيرا ، وبالاستناد إلى ان النموذج القانوني لجريمة السرقة في قوانيني العقوبات العربية عموما ، يقوم على عناصر واضحة في دلالتها ، لا تقبل بسط دلالاتها على سرقة المعلومات والمعطيات ، متمثلة بالسلوك الاجرامي المادي – (فعل الاخذ / الاختلاس) ، ومحل الجريمة المادي (مال منقول مملوك للغير) ، وباقتصار مفهوم الحيازة على ما يحتاز ماديا لا معنويا ، خلافا لمفهوم الحيازة في القوانين المدنية

3 -3 جرائم احتيال الكمبيوتر وأغراضها؟؟

الغش او الاحتيال او النصب تعبيرات يجري استخدامها بمعان مترادفة وان كانت تتمايز في الحقيقة ان من الوجهة اللغوية او الدلالات الاصطلاحية ، ويستخدم قانون العقوبات الاردني تعبير الاحتيال اما القانون المصري ، فيستخدم تعبير النصب وكلا القانونين لم يوردا تعريفا للاحتيال او النصب، وانما اوردا الافعال المكونة للجريمة في كل منها .

ويعرف الغش عموما ، بأنه " الخداع الذي يعمد اليه شخص للحصول من الغير بدون حق على فائدة او مزية ، ويعرفه (Jack Bologna) بأنه " خديعة معتمدة Intentional deception لاخر ترتكب عادة للحصول على منفعه اقتصادية او سياسية او اجتماعية غير مستحقة من الوجهة القانونية " [1]

أما غش الكمبيوتر / الحاسوب ، او كما يسميه البعض ، الاحتيال المعلوماتي او الاحتيال باستخدام الحاسوب ، فقد تباينت بشأنه التعريفات وتعددت ، واساس

[1] المرجع السابق ، ص 45 .

تباينها تحديد الافعال المنطوية تحت هذا الوصف ، فيعرفه الاستاذ الامريكي (T.Squires) بأنه " اساءة استخدام نظام الحاسوب ينطوي على حيله او خدعه مضلله " كما عرفته احدى الدراسات المسحية التي اجريت في امريكيا ، بأنه " فعل او مجموعة من الافعال غير المشروعة والمتعمدة التي ترتكب بهدف الخداع او التحريف للحصول على شئ ذي قيمة ، ويكون نظام الحاسوب لازما لارتكابها او اخفائها "[1] .

أما التعريف الذي يقره المجلس الاوروبي لغش الحاسوب ، فهو " تغيير او محو او كبت معطيات او بيانات او برامج الكمبيوتر او أي تدخل اخر في مجال انجاز او معالجة البيانات (من شأنه) التسبب في ضرر اقتصادي او فقد حيازة ملكية شخص اخر ، او بقصد الحصول على كسب اقتصادي غير مشروع له او لشخص اخر "[2] وفي معرض تحليله لهذا التعريف ، يشيراستاذنا كامل السعيد الى ان التعريف واسع النطاق " الى الحد الذي يستحل نطاقا واسعا من الانشطة بعضها لا يرتبط بالكمبيوتر " لكنه بنفس الوقت يحقق فائدة تتمثل " بتوجيه الانتباه الى الجانب الحاسم في الموضوع وهو التلاعب في البيانات بقصد الحصول على شكل من اشكال المصلحة المالية على حساب طرف اخرى " .

ولعل التعريف الذي وصفته لجنة تدقيق الحسابات بالمملكة المتحدة ، والذي ارتكزت عليه لجنة (اوديت) Audit commision البريطانية في دراساتها الاربعة بشأن غش الحاسوب يعطي دلالة دقيقة ومحددة لمفهوم غش الحاسوب ، فجاء في هذا التعريف أنه " كل سلوك احتيالي وخداعي مرتبط بالكمترة computerisation يهدف الشخص بواسطته الى كسب فائدة او مصلحة مادية "[3] . ، وعليه ، فان " جرائم احتيال الحاسوب ، تنصب على معطيات الحاسوب المخزنة في النظام المثلة لاموال او اصول او خدمات ، يهدف الجاني فيها الى تحقيق مكسب او مزيه ، وتتم بالتلاعب – وفق الدلالة التقنية الواسعة – بمعطيات الحاسوب المخزنة او نظام المعالجة الالية .

[1] المرجع السابق ، ص 46 .
[2] د. السعيد ، ورقة العمل ، المرجع السابق ، ص 4 .
[3] المرجع السابق ، ص 4 . ومصطلح الكمترة ، يستخدمه استاذنا كامل السعيد ولم نجده لدى غيره من الفقه العربي لتعريب كلمة computerisation وقد اشرنا سابقا انه استخدم لدى تعريب مؤلف غاري بيتر المشار اليه فيما تقدم ، ويستخدم الدكتور هشام رستم بديلا عنه تعبير " التحسيب الالكتروني " ومع ان الشائع في الدراسات التقنية استخدام تعبير الحوسبة الا ان استخدام تعبير الكمترة يفضل هذه الاستخدامات لدلالته التقنية الواضحة.

وصور احتيال الكمبيوتر عديدة بل وعصية في احيان كثيرة عن الحصر لتباينها من حيث وسائل الاعتداء التقني نفسه او تباينها من حيث البيانات محل الاعتداء ويمكن القول بايجاز انها كافة الوسائل التقنية للتوصل الى البيانات المالية او التي تتصل بحقوق مالية .

لقد كانت اكثر الوسائل التقنية رعبا فيما سبق من انشطة في بداية ظاهرة جرائم الكمبيوتر الوصول الى نظام احد المصارف عن بعد عبر الاتصال المباشر بشبكة البنك او عبر خطوط الهاتف التي تتيح مدخلا لشبكة نظام البنك (وما يتضمنه ذلك من استخدام كلمات الغير السرية ان كانت معلومة وتجاوز اجراءات الامن او تخمينها ان لم تكن كذلك) ، فيقوم الجاني بالعبث بالبيانات المالية اما باجراء التحويلات او بتغيير البيانات لكسب حقوق او الخلاص من التزامات ، او بزرع البرامج التي تحول آليا بعض المبالغ الى حسابات خاصة به او بشركائه ، او لاخفاء عملية اختلاس حصلت او غير ذلك من انشطة واغراض الدخول هذه ، وجامع هذه الانشطة ان الجاني يقوم باعمال احتيالية موجهة لنظام الكمبيوتر فيجني المنافع المادية عن طريق العبث بالبيانات او البرامج او حتى عمليات النظام ذاته. اما في الوقت الحاضر ، فان احتيال الانترنت المتمثل باستغلال مواقع الانترنت لجني مبالغ الاخرين عبر مشاريع وهمية لمنتجات او خدمات او من خلال الوصول الى ارقام بطاقات ائتمان الزبائن سواء بجمعها عند تلقي الموقع الوهمي لها او التوسل للوصول اليها من مواقع اخرى ومن ثم استغلالها في عمليات شراء غير مشروعة او الوفاء بمبالغ مقابل خدمات للجاني ، وانشطة التلاعب بالاسهم المالية وادارة المحافظ الالكترونية ومزادات البضائع على الانترنت ، تمثل الانشطة الاكثر رعبا لانتشارها الواسع ولما تلحقه بمواقع الانترنت والشركات القائمة عليها من مخاطر كبيرة وخسائر فادحة.

ولو رجعنا الى الدراسات المبكرة حول هذه الظاهرة لوجدنا مثلا ان الدكتور كامل السعيد يورد صورتين او شكلين للتلاعب بالمعطيات ، اولهما محاولة تأمين منفعة نقدية مباشرة ، كتحويل مبلغ من حساب شخص الى حساب الفاعل في البنك

وثانيهما تخلص الفاعل من الوفاء بدفعات مستحقة عليه ، ويمثل استاذنا على الصورة الثانية بحالة استعمال الفاعل دون ترخيص كلمة السر العائدة لطرف ثالث للتوصل الى استعمال حر لقاعدة البيانات بواسطة أي فواتير Bills يتم ارسالها للطرف الثالث " [1]. وكلتا الصورتان كما نلاحظ ، تتحقق فيهما المنفعة الاقتصادية للفاعل ، ومحلهما المعطيات المخزنة في الحاسوب المجسدة لاموال او اصول . فالهدف الرئيسي من التلاعب الذي تقوم به جريمة غش الحاسوب كما يقول د . هشام رستم " هو البيانات data (المعطيات) التي تمثل في نظم الحاسبات اموالا او اصولا او موجودات Assets " ورغم ان مختلف انواع المعطيات عرضة لجرائم غش الحاسوب الا ان هذه الجرائم تستهدف بشكل شائع ورئيسي حسب تحديد الفقيه Ulrich Seiber ما يلي : - - :

1 – البيانات الممثلة للمستحقات المالية والايداعات المصرفية وتقديرات الائتمان وحسابات ونتائج الميزانيات .

2 – حسابات المرتبات وأوامر الدفع وحساب التكلفة والنفقات وقوائم المبيعات وكشوف الاعانات الاجتماعية والضمان والتقاعد .

3 – انظمة التحويل الالكتروني للاموال والودائع المصرفية والبطاقات المالية بانواعها .

والجرائم التي تستهدف انظمة التحويل الالكتروني للاموال والودائع المصرفية تمثل باجماع الفقه اخطر جرائم غش الحاسوب ، ذلك ان الخسائر الكبيرة والهائلة الناتجة عن غش الحاسوب التي اشرنا لها سابقا ، تعد متواضعة مقابل احتمالات الخسارة الناتجة عن التلاعب بانظمة التحويل الالكتروني للاموال والودائع المصرفية ، وهذا يرجع الى المبالغ الهائلة المتجسده في هذه البيانات التي يجري نقلها بوقت قياسي والى شيوع استخدام تقنيات النقل الالكتروني للاموال التي تهيء نشوء مجتمع التعامل دون نقود ، لا في النطاق الوطني بل وعلى المستوى الاقليمي والدولي ايضا ، وكذلك لاتساع النشاط الاجرامي في هذا الميدان لما يجنيه الجناة من كسب

---

[1] المرجع السابق ، ص 4 .

وفير وبسبب تحققه ايضا في وقت قصير وتجاوزه الحدود الوطنية للدولة مما يشعر الجناة بالامان . وللتدليل الواقعي على مخاطر هذه الانشطة فانه في امريكا وحدها وعبر انظمة EFT كان يتم في مطلع التسعينات تداول معاملات مالية تقدر بنحو 900 بليون دولار يوميا ، وعلى مستوى البنوك فان بنكا واحدا مثل City Bank تعالج نظم حواسيبه معاملات ماليه تقدر بنحو 30 بليون دولار في اليوم الواحد لعملائه في مائة دولة .

اما عن الاساليب التقنية للتلاعب في معطيات الحاسوب الممثلة بذاتها للافعال المكونة للسلوك الاجرامي في جريمة غش الحاسوب فهي متعددة تبعا لتعدد الوسائل التقنية وتبعا لطبيعة المعطيات محل الاعتداء واكثر الفقه يعرض لها من واقع الحالات العملية ونتعرض لها تاليا بالذكر فقط : -

اولا : التلاعب في البيانات المدخلة Input Data

ثانيا : التلاعب في البرامج :

ثالثا : التلاعب في معطيات نظم الحواسيب عن بعد [1]:

واما عن خصائص الاحتيال التقليدي من الوجهة القانونية فانها: -

اولا :جريمة اموال . وثانيا ، تقوم على تغيير الحقيقة او تشويهها في ذهن المجني عليه . ولهذا يقترب الاحتيال من التزوير ، لكنه يتميز عن التزوير بانه وسيله للاعتداء على الملكية ، كما يتميز التزوير بطلب عناصر اخرى غير تغير الحقائق كوقوع التغير في سند او صك كتابي. ويقوم الركن المادي لجريمة الاحتيال – عموما – على فعل الخداع (السلوك الاجرامي) عبر واحد او اكثر من الصور التي يحددها القانون حصرا وعلى النتيجة الجرمية المترتبة عليه ، والمتمثلة بتسليم المجني عليه مالا الى المحتال . و علاقة السببية التي تربط السلوك بالنتيجة. ومن المسائل الهامة في مجال دراستنا هذه التاكيد على ان تحديد القانون للوسائل التي يقوم بها السلوك الاجرامي انما هو تحديد حصري .

[1] انظر بشان الحالات العملية المعروضة ، د. رستم ، المرجع السابق .

ويشترط لقيام جريمة الاحتيال ان يكون موضوع الاحتيال مالا مملوكا للغير وان يتوفر لموضوع الاحتيال طبيعة مادية ، وعلة ذلك – كما يقول الدكتور محمود نجيب حسني – " ان النتيجة الجرمية في الاحتيال هي التسليم الذي يفترض مناولة من المجني عليه او من يمثله او يعمل لمصلحته الى المحتال او من يعينه " وتتحقق كذلك الجريمة اذا انصبت على الاسناد التي تتضمن تعهدا او ابراء (وهذه الاسناد تتحقق لها الصفة المادية صكوك) اذا كانت بحيازة المجني عليه ، والتي تتصرف دلالتها في غير هذه الحالة الى الواقعة القانونية التي تنشا التعهد او تنهيه .

اما الركن المعنوي للاحتيال فيتخذ صورة القصد الجنائي ، ولا تقوم جريمة الاحتيال على نحو غير مقصود (بالخطا) ، وتتطلب جريمة الاحتيال - الى جانب القصد الناشيء عن علم الجاني بتوافر اركان الاحتيال واتجاه ارادته الى فعل الخداع وتسلم المال – قصدا خاصا يتمثل بنية الفاعل الاستيلاء على المال الذي تسلمه أي اتجاه نية الفاعل الى تملك المال الذي تسلمه .

في ضوء هذه المعالم الرئيسة بشان جريمة الاحتيال او النصب او الغش في القانون الجنائي ، هل تعتمد القواعد والاحكام التي تحكم هذه الجريمة في قوانين العقوبات الى المدى الذي يتيح انطباقها على جرائم غش الحاسوب ؟

تتحدد قابلية انطباق نصوص القانون الجنائي التقليدية المنظمة لجريمة الاحتيال او النصب على جريمة غش الحاسوب او الاحتيال باستخدام الكمبيوتر من خلال الاجابة على التساؤلات الرئيسة التالية :

1 -هل يعتد بالاحتيال الواقع على غير الشخص الطبيعي وتحديدا على الحاسوب بوصفة آلة ؟

2 - هل يعتبر تسليم الاموال عن طريق التحويل الاكتروني تسليما ماديا محققا للنتيجة الجرمية في جريمة الاحتيال ؟

3 - هل تعتبر الوسائل التقنية المكونة للسلوك في جريمة غش الحاسوب مما يدخل في مفهوم او دلالة الوسائل المعتبرة في القوانين الجنائية المكونة للسلوك الاجرامي في جريمة الاحتيال التقليدية؟

اما بالنسبة للتساؤل الاول ، فان سبب اثارته ان غالبية قوانين العقوبات تتطلب ان يقع الاحتيال على شخص طبيعي ، من قبيلها القانون الايطالي (وتستخدم تعبير فرد) والقانون السويسري والالماني والدنماركي واليوناني والياباني والفرنسي - مشروع عام 1958 - والمغربي والكويتي والقطري (وتستخدم تعبير الشخص) والاردني والفرنسي والمصري (وتستخدم تعبير الغير) ، فهل يمكن مد نطاق نصوص هذه القوانين وهي تستخدم هذه التعبيرات للانطباق على خداع الحاسوب او احتيال الكمبيوتر ؟

لا تسعفنا قوانين العقوبات العربية عموما للقول بامكان الانطباق ، اضافة الى عدم وجود احكام قضائية عربية – في حدود ما نعلم - تساهم في تبين اجابة على هذا التساؤل ، اما في الفقه والقضاء المقارنين فان خلافا ظهر بشان المسالة بين مؤيد ومعارض للتسوية في الحكم بين خداع الانسان والالة .

يرى Ulrich Seiber ان قابلية نصوص الاحتيال للتطبيق على الغش الذي يباشر على انظمة الحواسيب ، تتوقف على شرط مؤداه ، ان يكون الجاني قد خدع ايضا الشخص الذي يقوم بفحص البيانات ، فاذا لم يقم بذلك فان النصوص لا تنطق . ويعارض القاضي Mjaeger - في معرض ايضاحه لاسباب الحكم الذي اصدره والقاضي بعدم انطباق المادة 496 من قانون عقوبات لوكسمبرغ الخاصة بالاحتيال او غش الحاسوب ، الحجة التي تقول بان الآلة انما يستحدثها انسان ، وان هذا الاخير هو الذي يكون قد خدع لان آلته لا تكون قد استعملت طبقا للتصور الاصلي الذي وضع لها .

اما في المملكة المتحدة فان القضاء الانجليزي في قضية R.V,Gld عام 1981 – التي يعرض لها ويحللها على نحو تفصيلي الدكتور كامل السعيد -[1] قد اقام تسوية بين الالة والشخص في مسالة قبول السند المزور ، وسنتناول هذه القضية لدى بحثنا للتزوير. وخلافا لذلك حكم القضاء الانجليزي في قضية Moritzعام 1982 الخاصة بعائدات قيمة الضرائب الاضافية لاحدى الشركات ان الخداع

---

[1] د. السعيد ، ورقة العمل ، المرجع السابق ، ص 11 .

يتطلب عقلا بشريا يمكن خداعه والتحايل عليه ، هذا على الرغم من ان الماده 15 من قانون السرقة الانجليزي لعام 1968 التي تجرم الحصول بالخديعة على مال بحوزة الغير بنية حرمانه منه بصفة مؤبده ، والماده الاولى من قانون السرقة لسنة 1978 التي تجرم الحصول بالخديعة على خدمة ، يمكن تفسيرها على نحو متسع يسمح بتطبيقها على خداع نظام معلوماتي او آله .

والواضح انه في ضوء تحديد النصوص لصفة من يقع عليه الاحتيال بانه شخص او فرد طبيعي فان محاولات مد نصوص القانون لتشمل غش الحاسوب او خداع الاله تقف امامه عوائق قانونية حاده في مقدمتها مبدا حظر القياس في القانون الجنائي الموضوعي ، ومبدا الشرعية الراسخ .

وبراينا ، فان المبادئ الراسخة في القانون الجنائي ، ومقتضيات تعزيز النظام القانوني لمجابهة هذه الجرائم الخطرة ، وحقيقة ان النصوص التقليدية - حتى في الاحوال التي امكن تفسيرها على نحو واسع - لم تنه الجدل ولا التباين في حل مسألة التسوية بين خداع الانسان وخداع الالة ، كل ذلك يعزز القول بعجز النصوص الجنائية عن الانطباق على هذه الجريمة المستحدثة .

اما عن التساؤل الثاني والخاص بمدى اعتبار التحويل الالكتروني للاموال من قبيل التسليم المحقق لنتيجة السلوك في جريمة الاحتيال ، فان التعارض بشأنه اتخذ مدى واسع . ونجد لدى الفقيه او الاستاذ الواحد اكثر من موقف تتباين فيما بينها .

فالدكتور هشام رستم ، بالاستناد الى تحليل اتجاهات الفقه المقارن ، يرى وجوب التمييز بين حالتين : اولهما : اذا كان محل الاستيلاء نقودا او اصولا كالتوصل الجاني الى معرفة الرقم السري لصاحب بطاقة ائتمان مسروقة او معثور عليها ويستخدمها في سحب امواله من اجهزة الصرف الالي للنقود ، او كتلاعب الجاني في البيانات المدخلة او المخزنة في الحاسوب او برامجه كي يستخرج الحاسوب باسمه او باسم شركاه شيكات او فواتير بمبالغ غير مستحقة ليستولي عليها او يتقاسمها مع شركائه ، ففي هذه الحالات لا تثور مشكلة ، ويتحقق الاستيلاء او التسليم

بالمعنى المقرر قانونا بجريمة الاحتيال التقليدية . اما الحالة الثانية ، فاذا كان محل جريمة الاحتيال النقود الكتابية او البنكية (بيانات الارصدة في البنوك) ، كأن يتم الاستيلاء عليها عن طريق القيد الكتابي ومثالها تلاعب الجاني في البيانات المخزنة في الحاسوب او في برامجه كي يحول كل او بعض ارصدة الغير او فوائدها الى حسابه ، ففي هذه الحالة يجد الدكتور هشام رستم ان الحكم بشأن تحقق نتيجة الجريمة باستلام المال والاستيلاء عليه مرهون بنطاق النص القانوني ، ففي قوانين كل من المانيا واليابان لا تصلح النقود البنكية (بيانات النقود) محلا للاعتداء بالمعنى المقرر لمحل جرائم الاحتيال والسرقة . في حين انها – كما يذكر الدكتور هشام – تصلح في دول اخرى مثل كندا وهولندا وسويسرا وانكلترا ومعظم الولايات الامريكية ، وكذلك النمسا ، حيث قضت المحكمة العليا في الاخيرة بأن تعبير المال الوارد بالمادتين 133 عقوبات (الخاص بخيانة الامانة) و 134 عقوبات (الخاصة بالاحتيال) يشمل النقود الكتابية . ويلخص الدكتور هشام رستم ، الا انه وبالاستناد الى اعتبار التسليم غير متطلب له المناولة المادية حسب ما هو مستقر في الفقه المصري والفقه الفرنسي ، ولان محكمة النقض قد توصلت في العديد من احكامها الى ان " الدفع التي يتم عن طريق القيد الكتابي يعادل تسليم النقود، وسندالوجود اتجاه فقهي فرنسي يرى امكان تطبيق نص المادة 405 عقوبات من قانون العقوبات الفرنسي الخاصة بالاحتيال و(المطابقة للنص المصري تقريبا) على بعض صور جرائم غش الحاسوب واعتبار نتيجة الجريمة متحققة (والاستيلاء عن طريق تحويلات الكترونية تجري بين الحسابات ، فان اعتبار التسليم في جريمة غش الحاسوب متحققا لا يتعارض مع القانون المصري (الموافق لجميع القوانين العربية تقريبا) لان التسليم في جريمة النصب " يحققه وضع الشيء تحت تصرف الجاني بحيث يتمكن من حيازته بغير عائق ولو لم يستول عليه استيلاء ماديا " [1]

اما الدكتور جميل عبد الباقي[2] ، فانه يرى ان التسليم المادي يتحقق بالنسبة للجرائم الناشئة عن استخدام الحاسب الالي كاداة ايجابية (وتشمل عنده التدخل

[1] د. رستم ، المرجع السابق ، ص84.
[2] د. الصغير ، المرجع السابق ، ص 119 وما بعدها

في المعطيات بادخال معطيات وهمية ،او مزورة باستبدالها او محوها او التدخل في البرامج بتحويلها او التلاعب بها او تغيير برامج النظام بكافة صورة) وكذلك الجرائم الناشئة عن الاستخدام التعسفي لبطاقات الائتمان بجميع انواعها ففي هذه الجرائم يرى ان التسليم المادي يتحقق .ويدعم رايه بان محكمة النقض الفرنسية لم تشترط ان يكون هناك تسليم مادي لقيام النصب ، واكتفت بما يعادل التسليم ، وبان محكمة النقض الفرنسية اعتبرت ان الدفع الذي يتم عن طريق القيد الكتابي يعادل تسليم الاموال ماديا . وفي معرض عرضه للاتجاهات الفقه بشان مدى انطباق ما قررته محكمة النقض على جرائم الحاسوب . يذكر الدكتور جميل عبد الباقي ان البعض يرى امكان ذلك في حالات التدخل في البرمجة او المعطيات المقدمة للحاسوب التي تؤدي الى الغاء رصيد مدين واستنادا الى ان تحويل الاموال ايا كانت وسيلة التقنية قد تم بالقيد الكتابي بدون تسليم الاموال نقدا للجاني ، ويذهب الى تاييد هذا الراي واعتبار تحويل الاموال بالقيد الكتابي مما يدخل في مفهوم الجريمة الواردة في المادة 405 عقوبات فرنسي،

اما بشان الابراء ، فان القضاء الفرنسي قد حكم بتطبيق عقوبة النصب(الاحتيال)على احد الاشخاص لقيامه بادخال سيارته الى ساحة انتظار السيارات ولكنه بدلا من وضع النقود الاصلية المطلوبة في عداد الموقف وضع نقودا عديمة القيمة ، وحكم بذلك بتطبيق عقوبة النصب على الشخص الذي وضع قطعة معدنية عديمة القيمة داخل جهاز التلفون [1]، وتأسس الحكم في هاتين الجريمتين على ان الجاني في كل منهما ، وان كان لم يتسلم شيئا ماديا ، الا انه استطاع بتحايله ان يتخلص من المبلغ الذي كان يجب عليه دفعه ، وقد اتجه جانب من الفقه الى مد نطاق هذه الاحكام الى بعض صور السلوك في جريمة غش الحاسوب .

الا ان الدكتور جميل عبد الباقي لا يتفق مع هذا الاتجاه ولايرى انطباق حكم محكمة النقض على صورتي الاستخدام التعسفي لجهاز الحاسوب او الاستيلاء

---

[1] المرجع السابق ، ص 119 .

على البيانات اثناء نقلها لان الشخص لم يتسلم أي شيء مادي ، كما انه لم يحصل على اعفاء من الدفع او ابراء من الوفاء .

ونجد البعض ، دون بذل محاولة تحليل جريمة غش الحاسوب المستحدثة ، يتخذ حكما مطلقا بامكان تطبيق نصوص جريمة الاحتيال التقليدية بكافة اركانها وشروطها على جريمة غش الحاسوب ، لان الطبيعة التقنية لجرائم الحاسوب حسب هذا الرأي – لا تضيف جديدا في مجال الاحتيال التقليدي الا المجرد الوسيلة المستخدمة[1] .

اما التساؤل الثالث ، بشأن مدى شمول دلالات الوسائل الاحتيالية التي يقوم بها السلوك في جريمة الاحتيال التقليدية ، لاساليب التلاعب في المعطيات المكونة للسلوك الاجرامي لغش الحاسوب ، فقد كان محل نقاش وتعارض في الفقه الفرنسي واتيح للقضاء الفرنسي اصدار قرارات بشأنه .

يذكر الدكتور هشام رستم في هذا الصدد ان ما يظهر من اتجاهات الفقه الفرنسي بشأن هذه المسألة ان غش وخداع انظمة الحاسبات لسلب المال ، تتحقق به الطرق الاحتيالية بمفهومها المستقر (التقليدي) ككذب تدعمه اعمال مادية ووقائع خارجية ، حيث يتوافر فيه ، بجانب الكذب ، واقعة خارجية تؤيده هي ابراز او تقديم المستندات او المعلومات المدخلة الى الحاسوب ، ويؤيد الدكتور هاشم هذا الاتجاه بالاستناد الى ان جانبا من الفقه المصري قد وصف غش العداءات والاجهزة الحاسبة بأنه نوع من تجسيد الكذب الذي تتحقق به الطرق الاحتيالية . ويدلل على ذلك برأي الاستاذين الفاضلين ، احمد فتحي سرور ومحمود نجيب حسني .

والحقيقة ان الاستشهاد براي هذا الفقه – برأينا – ليس صائبا ، فان كان الاستاذ الفاضل محمود نجيب حسني ، قد قرر ان من يستعين بعداد او ساعة لاظهار ان الاستهلاك يزيد على الحقيقة ويطالب بناء على ذلك بمبالغ لا حق له فيها فان ذلك يقع في نطاق الخداع الذي يستعين الفاعل لتحقيقه بظروف خارجية من ضمنها الاستعانة بشئ ذي كيان مادي. هذا من جهة ، ومن جهة اخرى

---

[1] د. قشقوش ، السابق ، ص 152 .

فان الفقيه المذكور في معرض بيانه شرط توافر الصفة المادية لموضوع الاحتيال يعتبر الكهرباء مثلا ، ذات كيان مادي ، اضافة الى ان القضاء المصري استقر على انزال القوة المحرزة منزلة الاشياء المنقولة ، عوضا عن ان هذا التفسير مؤسس على ان فعل الاحتيال قد وقع على من قدمت له المستندات ، في حين ان الفعل قد وقع حقيقة على نظام الحاسوب .

ويرى كذلك الدكتور هشام رستم ، ويشاطره الرأي جانب من الفقه [1]، بالاستناد الى ما تقرر لدى جانب من الفقه الفرنسي وبعض احكام القضاء ، ان الطرق الاحتيالية (بالمفوم التقليدي متحققة باستخدام الجاني المستندات غير الصحيحة التي يخرجها الحاسوب بناء على ما وقع في برامجه او البيانات المخزنة داخله من تلاعب كي يستولى على اموال لا حق له فيها [2].

ومع الاقرار بأن المستندات المخرجة من الحاسوب ، اذا ما استعان بها الجاني في ارتكاب فعل الخداع ، تقوم بها جريمة الاحتيال ، فان هذا الاقرار يؤسس على ان الجاني استخدم مستندات ذات طبيعة مادية شأنها شأن كافة المحررات والصكوك التي يمكن استخدامها في فعل الاحتيال ، لكن ، اغفال عملية التلاعب بالبيانات التي يظهرها المستند المستخرج داخل نظام الحاسوب ، انما هو انكار لجريمة تامة حدثت وتحققت ، وما الاستعانة بالمستند الا من قبل استخدام مستند مزور اذا ما اكتملت عناصر اخرى ، تنشأ به جريمة استخدام مزور.

ويعترض جانب من الفقه على ادخال وسائل غش الحاسوب في نطاق الطرق الاحتيالية التقليدية ، استنادا الى ان الادعاءات الكاذبة وفق ما بينته الاحكام الفرنسية ، تنطوي بالضرورة على علاقة مباشرة بين شخصين (المحتال والمخدوع) وهو ما ينتفي في حالة مباشرة الطرق الاحتيالية في مواجهة آلة ، مثل الحاسوب ويرى بعض الفقه المعارض بالمقابل بأن خداع الالة ممكن تقبله على اساس انه يوجد خلف الالة انسان . وقد تضاربت احكام القضاء المقارن بشأن هذه المسألة ، خاصة في فرنسا ، ولا يتسع المقام لتناولها ، غير ان المشرع الفرنسي حسم هذا التعارض –

[1] د. قشقوش ، السابق ، ص 28.
[2] د. رستم ، السابق ، ص 270.

من بعض النواحي – لاصداره قانونا خاسا ببعض جرائم الحاسوب (قانون 1988 المعدل 1994).

وما اصدار غالبية الدول – خاصة تلك التي تزداد فيها جرائم الحاسوب على نحو ملحوظ – لقوانين خاصة او تعديل قوانينها لتجريم احتيال الكمبيوتر ، الا تأكيد على ادراك الطبيعة الخاصة لهذه الجرائم ، وتحديدا محل الاعتداء ، وخصائصها المميزة ، وهذا بدوره يمثل دلالة قوية ، وان كانت غير مطلقة ، على عدم صواب الاتجاهات المتحمسة لمد نطاق النصوص الجنائية التقليدية على جرائم الحاسوب خاصة اذا كان البعض من اصحاب هذه الاتجاهات لا يرى ان هذه الجرائم تضيف جديدا على كثير من النصوص التقليدية الا من حيث وسيلة الجريمة .

3 -4 جرائم التزوير المعلوماتي ؟؟ [1]

التزوير forgery بشكل عام ، " هو تغيير الحقيقة ايا كانت وسيلته وايا كان موضوعه " [2] وهو يتسع للعديد من الجرائم التي نصت عليها قوانين العقوبات . اما التزوير في المحررات ، فهو حسب تعريفه المستقر في الفقهين الفرنسي والمصري " تغيير الحقيقة في محرر باحدى الطرق التي نص عليها القانون ، تغييرا من شأنه احداث ضرر مقترن بنية استعمال المحرر المزور فيما اعد له" [3] . وقد عرف قانون العقوبات الاردني التزوير بأنه " تحريف مفتعل للحقيقة في الوقائع والبيانات التي يراد اثباتها بصك او مخطوط يحتج بهما نجم او يمكن ان ينجم عنه ضرر مادي او اجتماعي" (مادة 260) .

وبالرجوع الى قوانين العقوبات العربية ، نجدها في معرض تجريم التزوير عموما وتزوير المحررات على وجه الخصوص قد نصت على تجرم العديد من الصور ، فقد نص قانون العقوبات الاردني – على سبيل المثال - على هذه الجرائم في الفصل الثاني من الباب الخامس تحت عنوان الجرائم المخلة بالثقة العامة (المواد 260 –

---

[1] انظر في تفصيل ذلك ، د. حسني ، القسم الخاص ، المرجع السابق ،وكذلك المستشار مصطفي مجدي هرجه، التعليق على قانون العقوبات في ضوء الفقه والقضاء، الطبعة الثانية، مطابع روز اليوسف، جمهورية مصر العربية، 1992.

[2] د. حسني ، القسم الخاص ، المرجع السابق ، ص 192

[3] السابق ، ص 215 .

272) ، وساوى في العقوبة بين مرتكب التزوير ومستعمل المحرر المزور . وكذلك فان قانون العقوبات المصري نظم جرائم التزوير في الباب السادس عشر من الكتاب الثاني تحت عنوان التزوير (المواد 206 – 227) . ويهمنا في هذا المقام الاشارة الى ان المشرع المصري قد جرم استعمال المحررات المزورة ، لكنه نهج نهجا مختلفا عن المشرع الاردني بشأن العقوبات ، اذ تتعدد العقوبات فيما بين جرائم تزوير المحررات تبعا لنوع المحرر محل التزوير ، وتتباين عن عقوبات جرائم استعمال المحررات كما انها تتباين في الطائفة الاخيرة.

وتتشابه جرائم التزوير مع جرائم الاحتيال من حيث قيامهما على تغيير الحقيقة غير انهما تختلفان من زوايا متعددة ، اهمها ان جريمة تزوير المحررات لا بد ان تقع على محرر، ولا يشترط ذلك في جريمة الاحتيال . وغالبا ما تجتمع جريمتا التزوير والاحتيال ، ونكون بذلك امام حالة التعدد المادي للجرائم .

وتقوم جريمة التزوير على ركنين ، مادي ومعنوي ، وان كان جانب من الفقه [1] يجعل من بعض عناصر الركن المادي ، كالضرر ، ركنا مستقلا بذاته . اما الركن المادي فيقوم على ثلاثة عناصر: - تغيير الحقيقة ، وان يكون التغيير قد تم باحدى الطرق المحددة حصرا في القانون ، واخيرا ، ان يترتب على تغيير الحقيقة ضرر . وهذا العنصر الاخير هو ما ثار بشأه الخلاف حول موقعه ، الا ان السائد في الفقه اعتباره عنصرا من عناصر الركن المادي ، وتغيير الحقيقة يمثل السلوك الاجرامي الذي يقوم به التزوير فاذا انتفي انتفت الجريمة . ولا يشترط ان يكون التغير كليا ، أي ابدال كل البيانات بما يخالف الحقيقة ، ويكفي ان يكون تغيير الحقيقة جزئيا او نسبيا والمستقر في الفقه ان المقصود في التزوير ، ليس تغيير الحقيقة الواقعية المطلقة ، وانما تغيير الحقيقة النسبية .

وتغيير الحقيقة وحده ، غير كاف في القانون ، وانما يلزم ان يتم باحدى الطرق المحددة حصرا في القانون ، والتي تقسم عموما الى طرق مادية تنال مادة المحرر وشكله وطرق معنوية ، تنال مضمون المحرر او ظروفه او ملابساته دون المساس بمادته او شكله

[1] انظر في تفصيل هذه الاتجاهات د. حسني ، السابق ، ص 193 وما بعدها .

ويكتمل الركن المادي بتحقق الضرر الناتج عن تغيير الحقيقة ، والضرر كما يعرفه الفقيه محمود نجيب حسني ، " اهدار حق واخلال لمصلحة مشروعة يعترف بها القانون ويكفل لها حمايته"[1] وبانتفاء الضرر ينتفي التزوير ، وللضرر انواع متعددة قد يكون ماديا او معنويا او ضررا احتماليا او ضررا اجتماعيا.

وموضوع جريمة التزوير ومحلها ، المحرر ، ولا وجود للتزوير اذا لم ينصب على تغيير الحقيقة في محرر ، ويعرف المحرر بانه " مجموعة من العلامات والرموز تعبر اصطلاحا عن مجموعة مترابطة من الافكار والمعاني الصادرة عن شخص او اشخاص معينين " [2] وهو في جوهره كتابة مركبة من حروف وعلامات تعبر عن معنى او فكرة معينة ، وحسب الاتجاه التشريعي والفقهي الراجح ، يفترض امكان ادراك مادة المحرر بالقراءة البصرية [3] وان ينتقل معنى الرموز والعلامات عن طريق المطالعة والنظر ، ومن المسائل الهامة المفترض الاشارة اليها ، والمتصل بموضوع وهدف دراستنا ، ان الفقه متفق على ان فكرة المحرر ، تفترض امكان استشفاف دلالة رموز المحرر بالنظر اليها ، ولذلك – وكما يقول الاستاذ محمود نجيب حسنى – لا يعتبر من قبيل المحررات ، الاسطوانة او شريط التسجيل الذي سجلت عليه عبارات ايا كانت اهميتها القانونية ، وكذلك ما يدخل على الصوت الذي يحمله من تشويه [4].

والعنصر الاخر الهام من عناصر المحرر محل التزوير ، اضافة الى اتصاف علاماته ورموزه بثبات نسبي ، هو ان فكرة المحرر ، توجب ان يكشف عن شخصية محرره ، وهذا العنصر مما يتصل بالوظيفة الاجتماعية للمحرر ، والمستقر فقها ان يكون المحرر معبرا عن فكرة بشرية . ولعل العناصر التكوينية لمحل جريمة التزوير التقليدية – المحرر – هي العامل الحاسم في منع انطباق نصوص جريمة التزوير على تزوير معطيات الحاسوب كما سنرى .

أما الركن المعنوي لجريمة التزوير ، فيتخذ صورة القصد الجنائي . ولا يكفي فيه القصد العام الذي يقوم على علم المتهم بأركان الجريمة ، واتجاه ارادته الى الفعل

---

[1] السابق ، ص 251 .
[2] المرجع السابق ، ص 247 .
[3] د. رستم ، السابق ، ص 326 .
[4] د. حسني ، السابق ، ص 247 .

المكون لها وتحقيق نتيجته ، بل تتطلب هذه الجريمة توافر قصد جنائي خاص ، يتمثل بنية استعمال المحرر المزور فيما زور من اجله وعلى هذا فان القصد الجنائي في جريمة التزوير يعرف على نحو غالب لدى الفقه والقضاء بانه " تعمد تغيير الحقيقة في محرر تغييرا من شانه ان يسبب ضررا وبنية استعمال المحرر فيما غيرت من اجله الحقيقة " [1].

هذا عرض موجز ومكثف لماهية واركان جريمة التزوير ، ويثور السؤال ، هل يمكن تطبيق نصوص القانون الجنائي على انشطة تزوير معطيات الكمبيوتر ؟!

بالرغم من ان غالبية الدول حسمت موقفها لجهة عدم انطباق نصوص التزوير على تزوير المعطيات واتخذت تدابير تشريعية لتجريم تزوير المعطيات وتوفير اداة قانونية لمكافحتها الا ان ثمة دول لم تنح هذا المنحى ولا يزال النقاش القديم الجديد بشان مسألة انطباق نصوص تجريم التزوير في المحررات على تزوير البيانات المخزنة في نظام الحاسوب قائما ، وهذا الجدل يتجاذبه رايان ، احدهما - وهو الرأي الراجح بفعل تبنيه من قطاع واسع من الفقه ، والمعزز ايضا ببعض باحكام قضائية ، وبفعل تبنيه في التشريعات الجنائية الحديثة في القانون المقارن - يقوم على ان التزوير في معطيات الحاسوب ، لا يدخل تحت نطاق النصوص التقليدية . اما الرأي الثاني فيرى امكان تطبيق النصوص الجنائية المنظمة لجريمة التزوير التقليدية على جرائم تزوير الكمبيوتر . وليس المقام عرض وتقدير هذين الاتجاهين — وهو ما قمنا به تفصيلا في مؤلفاتنا المشار اليها في هذه الورقة — ونكتفي في هذا المقام ببيان خلاصة تقدير هذه الاتجاهات وفق ما سبق لنا التوصل اليه في دراستنا .

اننا وبالاستناد الى : -

1 - انعدام وجود العناصر الرئيسة لمحل جريمة التزوير التقليدية (المحرر) في معطيات الحاسوب وتحديدا ،عنصر الكتابة المادية ، وعنصر ادراك مضمون المحرر بالنظر ، وعنصر التعبير عن الفكرة البشرية وعلاقة الشخص بالمحرر .

---

[1] السابق ، ص 271 .

2 - وسندا الى تاييد غالبية الفقه القانوني من مختلف النظم عدم انطباق نصوص تجريم التزوير التقليدية على تزوير معطيات الحاسوب. وتعزز وتايد هذا الاتجاه باحكام قضائية في فرنسا وامريكا وبريطانيا وغيرها من النظم المقارنة .

3 - وسندا لتدخل مشرعي العديد من الدول للنص على هذه الجرائم المستحدثة من جرائم التزوير اما بنصوص خاصة او بتعديل النصوص التقليدية للتزوير، كما هو الشان في كندا حيث عدل تعريف الوثيقة document في قانون العقوبات عام 1985 ليشمل بالاضافة الى الورق أي مادة material يتم عليها تسجيل او حفظ أي شيء يمكن قراءته او فهمه من قبل الانسان او نظام الحاسوب او أي جهاز اخر وكذلك في استراليا حيث اضيفت المادة 276عام 1983 لقانون العقوبات ونصت صراحة على معاقبة "كل من حرف او زور او محا او اتلف بطريقة غير مشروعة وبقصد الغش ، اية مادة لمعالجة البيانات ، وكذلك جرمت استخراج او انتاج معلومات غير صحيحة عن طريق المعالجة الالية واستخدامها او التصرف فيها على انها صحيحة اضرارا بالغير او بقصد حمل او اقناع الشخص للقيام بفعل على اساس انها صحيحة" وكذلك في المانيا ، حيث تضمن القانون الثاني لمكافحة الجريمة الاقتصادية لعام 1986 نصا في المادة (269) يقضي بتوقيع عقوبة الحبس لمدة لا تزيد على خمس سنوات او الغرامة على كل من يقوم بقصد الخداع في تعامل قانوني ، بتخزين او تغيير بيانات اذا ما استنسخت بهذا الشكل انتجت مستندا غير اصلي او مزور وكذا كل من يستخدم هذه البيانات المخزنة او المحرفة " وكذلك في فرنسا ،حيث جرم المشرع الفرنسي في الفقرتين (6،5) من من المادة 462 من قانون 1988 المشار اليه سابقا ، تزوير المستندات المعالجة اليا او استخدام هذه المستندات.

فان نصوص التجريم التقليدية المنظمة لجرائم التزوير ،غير قابلة للانطباق على جرائم تزوير معطيات الحاسوب بدلالتها الواسعة ، مما يستدعي تدخلا تشريعيا في البيئة العربية لمواجهة هذه الجرائم ، صيانة لاسس ومباديء النظام القانوني وكفالة للحقوق التي تهددها - على نحو جدي وخطر - هذه الانشطة الجرمية المستجدة .

3 -5 جرائم تدمير المعطيات - الفيروسات والديدان والقنابل المنطقية والموقوتة؟؟؟

ننطلق بداءة من الاشارة الى ان الاتلاف في نطاق جرائم الحاسوب وفقا لمحددات هذه الجرائم التي درسناها فيما تقدم هو الاتلاف الذي ينصب على معطيات الحاسوب من بيانات ومعلومات وبرامج ، ونعيد التاكيد هنا ان الاتلاف المنصب على الكيانات المادية للحاسوب - شانه شان سائر الجرائم الواقعة على هذه الكيانات كالسرقة وخيانة الامانة ، لا يعيق انطباق نصوص القوانين التقليدية عليه عائق .

وتنصب اساليب الاتلاف التقنية في ميدان نظم الحواسيب على المعطيات بدلالتها الواسعة ،البيانات والمعلومات المخزنة في نظم الحواسيب المختلفة والبرامج وكذلك المعطيات المتبادلة بين شبكات الحوائيب وعبر شبكات المعلومات ، وينتج عن هذه الاساليب اما محو كلي للمعطيات او تشويه من شانه اتلاف اجزاء منها ، يمنع امكان استخدام النظام على نحو طبيعي بفعل غياب تكامل عناصر ومعطيات النظام المتطلبة اصلا لسلامة عمله.

وتتخذ اساليب اتلاف المعطيات عموما احد صورتين يندرج في نطاقهما العديد من الوسائل التقنية، اولهما،محو او تشويه البيانات المخزنه في نظم الحواسيب من خلال التوصل غير المرخص به مع النظام ، وقد تناولنا الوسائل التقنية وانشطة التوصل غير المرخص به مع نظام الحاسوب وخاصة الاعتماد على وسائل الاتصال والتشويه ، ولا نكرر ما ذكرناه في هذا المقام ، ونكتفي بالقول ان انشطة التوصل ومن ثم العمل مباشرة على اتلاف المعطيات ، اقل خطورة من وسيلة التدمير بواسطة الفيروسات التي تنصب بشكل رئيس على البرامج التطبيقية والبيانات المخزنة في الملفات .

اما الوسيلة الثانية والذي ارتبط بها مفهوم ودلالة اتلاف معطيات الحاسوب فهي وسيلة نشر البرامج الخبيثة والضارة ، واشهرها الفيروسات ، ولعل هذه الوسيلة هي من اكثر ما يتردد الحديث بشانها متصلا بجرائم الحاسوب ، ومن اكثر الظواهر معالجة على مستوى الدراسات التقنية القانونية ، كما انها المادة الغنية للاخبار

المعلوماتية وتقارير امن المعلومات التي تنشر في مختلف وسائل الاعلام وفي مقدمتها الانترنت .

وبرامج الفيروسات خضعت ولما تزل لتفسيرات متباينة في اطار الدراسات التقنية وتعددت الاتجاهات – العصية عن التقصي – بشان اثر برامج الفيروسات من حيث نطاق الاتلاف الذي تلحقه والمناطق التي تصيبها هذه البرامج في نظم الحواسيب وانواعها ، والكثير الكثير من المسائل المتصلة بها ، وهذا كله يرجع في الحقيقة الى التطور الهائل والسريع في تقنيات برمجة الفيروسات ، ولا ادل على مدى هذا التغير من اتجاه عشرات الدراسات الى الحديث عن فيروسات تقليدية وفيروسات مستحدثة ، رغم ان هذه الظاهرة لم تبرز للعيان الا في الثمانيات بشكل ملحوظ .[1]

وتقوم جريمة اتلاف الاموال المنقولة وغير المنقولة في القانون الجنائي ، شانها شان سائر الجرائم، على ركنين: - الركن المادي المتمثل بفعل الاتلاف والذي يتخذ صورا عديده حسب النص القانوني ، ففي القانون المصري (مادة 361 عقوبات) يقوم الفعل بتخريب المال او اتلافه او جعله غير صالح للاستعمال او تعطيله ، وينصب السلوك الاجرامي على الاموال المنقولة وكذلك الاموال غير المنقولة المملوكة للغير . والركن الثاني للجريمة هو الركن المعنوي ، ويتخذ صورة القصد الجنائي العام بعنصرية العلم والادارة وقد قضت محكمة النقض المصرية[2] "بان القصد الجنائي يتحقق في جريمة الاتلاف متى تعمد الجاني ارتكاب الفعل المنهي عنه

---

[1] من المصادر الحديثة والمتجددة انظر الدليل الشامل للفيروسات :-

, CIAC-2301, May 21, Gizzing H. Khanaka , William J. Orvis ,Virus Information Update 1998 , Lawrence Livermore National Laboratory .

وكذلك المقالة الهامة Why Viruses Are and Always will be a للدكتور *Richard Ford.* .

ومن المؤلفات والمقالات القديمة نسبيا – مطلع التسعينات - انظر للمؤلف ، الرقم الأسود لجرائم الكمبيوتر، مجلة حماية الملكية الفكرية الصادرة عن المجمع العربي لحماية الملكية الصناعية (ميونيخ - ألمانيا)، العدد (38) الربع الأول، 1994. ومنشور ايضا في جريدة الأسواق - ملحق الكمبيوتر والتكنولوجيا، سلسلة الجريمة والكمبيوتر، عمان عدد (149)، 18 كانون أول 1993 ،وفايروسات الحوسبة، حقيقتها، ظواهرها، علاجها، مجلة حوسبيات، عمان، السنة (1) العدد (1) اب 1992.وفيروس يهدد الكمبيوتر، مجلة المهندس الأردني، العدد (44) السنة (23) أيول 1989 .ورونالد ميكلين، دليل الوقاية من فيروس الحواسيب، ترجمة مركز التعريب والبرمجة، الدار العربية للعلوم، الطبعة الأولى، بيروت، 1992. وجيل جديد من الفيروسات الخفية، مجلة الكمبيوتر والتكنولوجيا، (أبو ظبي) العدد (19)، يونيو 1993. وحسام سعفان، وباء فيروس الكمبيوتر يجتاح العالم، مجلة الكمبيوتر والأعمال، (مصر)، العدد الثاني السنة (4) فبراير 1991. والفيروسات، مجلة المعلومات، (سوريا)، عدد (5)، شباط 1993.ووليد الأصفر، عيادة الفيروسات، نشرة الحاسوب، اصدار الجمعية الأردنية للحاسبات العدد (10) آب 1992 والعدد (9) نيسان 1992، والعدد (13) أيار 1993.

[2] مشار الى هذا القرار في مؤلف د. رستم ، السابق ، ص 321.

بالصورة التي حددها القانون واتجهت ارادته الى احداث الاتلاف او التخريب وعلمه بانه يحدثه بغير حق" .

وجريمة الاتلاف من الجرائم المادية التي تتطلب تحقق نتيجة تتمثل باتلاف المال باحدى الصور مما يحلق اضرارا بالغير ، وهي جريمة وقتية ، وما يعنينا في مقام الدراسة التاكيد على ان النصوص التقليدية لجريمة الاتلاف تنظم افعال الاتلاف المنصبة على الاموال ذات الطبيعة المادية منقولة كانت ام غير منقولة ، فقانون الضرر الجنائي الانجليزي على سبيل المثال الصادر عام 1971 يعرف كلمة الاموال المعتبرة محلا لجريمة تخريب والحاق الضرر التي نص عليها في المادة (1/1) بانها "الاموال ذات الطبيعة الملموسة - المادية tangible nature سواء كانت اموالا عقارية ام شخصية " وبالتالي فان الاتلاف يكون ذا طبيعة مادية لان المشرع لا يحمي بتجريمه افعال التخريب والتعييب والاتلاف حق الملكية بوصفه حقا عينيا مجردا بل يحميه بوصفه تسلطا ماديا من المالك على ما يملك مما يفترض معه تجسد محل هذا الحق في كيان مادي ، وعليه لا تدخل الامورالمعنوية (ويسميها البعض المال المعنوي) في نطاق الاموال القابلة لان تكون محلا لجريمة الاتلاف [1].

امام هذه المعالم الرئيسة لقوام جريمة الاتلاف التقليدية ، يظهر لنا بشكل اولي ان النصوص الناظمة لهذه الجريمة في القوانين التقليدية ، لا يمكن ان تنطبق على اتلاف معطيات الحاسوب / ولابراز هذه النتيجة نتعرض تاليا لاتجاهات الفقه وموقف القانون المقارن والمسائل التي اثيرت بشانها : -

اولا : فيما يتصل باتلاف الكيانات المادية للحاسوب ، لا شبهة في امكان تطبيق النصوص التقليدية لأننا أمام محل للجريمة يتصف بالطبيعة المادية ، فاذا ما اكتملت عناصر جريمة الاتلاف وتحققت أركانها أمكن تطبيق النص عليها .

ثانيا : أما فيما يتصل باتلاف المعطيات المخزنه داخل الحواسيب أو المنقولة عبر شبكات المعلومات ، سواء أكانت بيانات أم معلومات أم برامج ، فان الفقه السائد [2] يقرر عدم امكان تطبيق نصوص جريمة الاتلاف على الأنشطة التي تنطوي عليها

[1] السابق ، ص 312 .
[2] انظر الاراء الفقهية لدى د. رستم ، المرجع السابق ، ص 314 وما بعدها .

هذه الجرائم ، بالاستناد الى انتفاء الصفة المادية عن النبضات الكهربائية التي تختزن البيانات والبرامج على هيئتها ، والاستناد الى ان البيانات والمعلومات لا تعتبر مالا بحد ذاتها وان كانت تجسد أو تمثل أموالا أو أصولا .

ويمكن التوصل ايضا لهذه النتيجة عبر تحليل احكام القضاء الانجليزي ، تحديدا حكمه في قضية Cox. V. Rily وقضية Her Majesty. V. Wilson ، حيث يظهر التحليل التفصيلي لهذه الاحكام ، ان القضاء الانجليزي وان كان قد حكم بالادانة على افعال الاضرار بالبرامج والبيانات تأسيسا على الاضرار الجنائي الناجم عن الفعل او على الضرر الكيدي ، الا ان هذه القرارات لم تلق القبول ، واوصت لجنة القانون بوجوب تعديل قانون الضرر الجنائي (1971) بانشاء جريمة جديدة مستقلة وخاصة بالحاسوب . وقد تحقق ذلك بصدور قانون اساءة استخدام الحاسوب لسنة 1990 ، وفي اول تطبيق لاحكامه ، قضت محكمة الاستئناف في حكم لها عام 1991 على نحو صريح وواضح ، وبدون ادنى مواربة ، ان جريمة الضرر الجنائي يمكن تطبيقها حيثما يقع الضرر على بيانات الحاسوب [1].

ثالثا : اما فيما يتصل باتلاف الدعامات المادية التي تحتوي البيانات والبرامج، مثل الاشرطة والاسطوانات المغنطة ، من حيث شمول الاتلاف في هذه الحالة للمادة الموجودة عليها (المعطيات غير المادية) فانها قد اثارت خلافا فقهيا بشان تحديد الوقف منها . فقد ذهب جانب من الفقه ، وبالاستناد الى نصوص التجريم التقليدية المنظمة لجريمة الاتلاف في قوانين بعض الدول ، كالنمسا والدنمارك والمانيا الاتحادية واليونان وايطاليا وهولندا واسكتلندا [2]، الى ان نصوص تجريم الاتلاف ينطوي في نطاقها اتلاف او تعييب البرامج والبيانات في حد ذاتها ، طالما كانت هذه البرامج والبيانات مسجلة على دعامة مادية ، لان مرتكب الفعل اما ان يتلف في هذه الحالة الدعامة المادية نفسها او يتسبب في الحاق ضرر وظيفي بها وهو ما يمكن ان تقع به جريمة الاتلاف .

---

[1] د. السعيد ، ورقة العمل ، المرجع السابق ، ص 15 .

[2] انظر Ulrich Sieber السابق ، ص 211 وما بعدها ، وكذلك ، رستم ، السابق ، ص 312 وما بعدها .

وهذا الجانب من الفقه يتبنى موقف الاتجاه السائد بشان اتلاف المعطيات المخزنة او المنقولة المشار اليه في البند الثاني اعلاه . الا ان جانبا اخر من الفقه ، كبعض الفقه في بلجيكا وفنلدا واستراليا وامريكا ، لا يوافق على هذا الاتجاه بالاستناد الا ان التدخل في وظائف واستخدامات الدعامات المادية المسجل عليها بيانات او برامج لا يعتبر اتلافا لها .

وعلى الرغم من عدم حدة الخلاف بين الرأيين ، باعتبار ان الاتفاق بينهما قائم على عدم تطبيق نصوص التجريم التقليدية على اتلاف المعطيات لغياب الطبيعة المادية للمعطيات ، وانحصار الخلاف حول مدلول اتلاف الدعامة المادية ، أينظر اليه مجردا عن محتواها ام يؤخذ محتواها بعين الاعتبار ؟ فان هذه المسألة براينا من المسائل المتصلة بتقدير البيانات ، فاعتبار البيانات مالا ، يحقق تطبيق النص طالما تحقق بالاساس وقوع الفعل على كيان مادي، اما عدم اعتبار البيانات مالا بذاتها – كما هو الصحيح براينا عند تخلف النص على ذلك – فانه يقصر تطبيق النص على اتلاف الكيان المادي ، وسندا له تتحدد قيمة الضرر الناتج ، ولا اعتبار للبيانات المخزنة .

ولما كان السائد فقها ، عجز النصوص التقليدية عن الاحاطة بجرائم اتلاف المعطيات ، فقد تدخل المشرع في العديد من الدول للنص على هذه الجرائم المستحدثة ، اما بتجريم اتلاف المعطيات كافعال مستقلة عن الاتلاف المعروف في القانون التقليدي ، او تعديل نصوص الاتلاف بالنص صراحة على التسوية في الحكم بين اتلاف الاموال المادية واتلاف المعطيات ، ومن الامثلة على القوانين المقارنة التي جرمت تزوير الكمبيوتر ، القانون الفدرالي الامريكي بشان غش واساءة استخدام الحاسوب لسنة 1984 في المادة 1030 / أ / 3 ، وقوانين معظم ولايات امريكا كما اشرنا فيما تقدم . وكذلك القانون المعدل لقانون العقوبات الكندي لعام 1985 حيث نص في المادة 387 على معاقبة كل من يقوم عن عمد Wilfuly ودون مبرر قانوني Without legal justiication او عذر excuse باتلاف او تشويه البيانات او محوها او جعل البيانات بلا معنى او بدون فائدة او غير مؤثرة او فعالة او باعاقة

او مقاطعة الاستخدام المشروع للبيانات او منع من له الحق في الوصول الى البيانات من الوصول اليها . وكذلك عاقب المشرع الالماني في المادة 303 من قانون العقوبات المعدلة بموجب القانون الثاني لمكافحة الجريمة الاقتصادية عام 1986 ، كل من محا او ابطل او جعل غير نافع او احدث تغييرا في البيانات بصور غير مشروعة ، بالحبس لمدة لا تزيد عل عامين او الغرامة ، وشدد العقوبة لتصل الى خمس سنوات او الغرامة اذا ارتكبت هذه الافعال على بيانات ذات اهمية اساسية لقطاع الاعمال او السلطات الادارية ، او في الحالات التي تؤدي هذه الافعال الى تدمير او اتلاف او ازالة او تعديل نظام حاسوب او دعامة بيانات او جعلها غير مفيدة. وكما اشرنا سابقا ، جرم المشرع الفرنسي في قانون 1988 محو وتعديل البيانات المعالجة اليا او التدخل في طرق معالجتها (م 4/462) وعاقب عليه بالحبس مدة تتراوح بين ثلاثة اشهر وثلاث سنوات او بالغرامة . وجرم كذلك تعطيل او افساد (عن عمد) تشغيل نظام المعالجة الالية للبيانات وعاقب عليه بذات العقوبة المشار اليها (م 3/462) .

3 -6 انشطة الانترنت غير المشروعة المتصلة بالمحتوى المعلوماتي والبريد الالكتروني وأنشطة التصرف المعلوماتي غير القانوني ؟؟

اشرنا فيما سبق الى هجمات انكار الخدمة التي تستهدف تعطيل مواقع الانترنت والنظم الخادمة لها عبر ضخ كميات هائلة من الطلبات والرسائل في وقت واحد لا لشيء الا لاسقاط النظام وتحويله الى عاجز عن العمل او للمساس بتكاملية وصحة المعطيات والمعلومات . كما اشرنا لانشطة اثارة الاحقاد والاساءة للافراد والتحرش بهم ومضايقتهم وابتزازهم عبر الرسائل الالكترونية ، وكذلك نسبة الاساءات الى اشخاص آخرين لا علم لهم بها باستغلال اسمهم او عناوينهم الالكترونية، وانشطة مواقع الحوار غير القانونية ، وارسال رسائل البريد الالكتروني الدعائية دون طلب وبشكل يزعج المتلقين . كما اشرنا الى استغلال مواقع الانترنت للتصرفات غير القانونية وغير المشروعة كنشر المواد الاباحية وادارة انشطة المقامرة او القيام باشطة الغسيل الالكتروني للاموال ، واشرنا ايضا الى ظاهرة الارهاب

الالكتروني وتحديدا استغلال الانترنت للوصول الى النظم والشبكات المحلية لاجل الحاق الاذى والخوف والتهديد بافراد المجتع ومؤسساته الحيوية. وهذه الانشطة بمعمومها هي ما ارتأينا ان نضعها في نطاق وتحت عنوان انشطة الانترنت غير المشروعة المتصلة بالمحتوى المعلوماتي الضار ، وانشطة التصرف المعلوماتي غير القانوني او غير المشروع ، ولكن هذا لا يعني اننا نخرج هذه الانشطة من تصنيفاتها التي اوردناها سابقا ، لكننا وجدنا ان الجامع بينها استغلال الانترنت ذاتها لارتكاب هذه الانشطة او المساس بمواقع المعلومات على الانترنت وامن البريد الالكتروني او استثمار مواقع الانترنت والبريد الالكتروني في انشطة غير مشروعة .

3 -6 -1 تحديات التصرف غير القانوني على شبكة الانترنت

ان الانترنت تغير بشكل سريع ومتنام طريقة الاتصال والتعليم البيع والشراء وتلقي الخدمات ، وبقدر ما تقدم خدمة وفوائد للمجتمع فان الاعتماد عليها في خدمة الانشطة غير القانونية يتزايد يوما بعد يوم ، ويتزايد استخدام الانترنت في التصرفات غير القانونية شأنه شأن ذات التصرفات غير القانونية في العالم الحقيقي . ان استراتيجيات وسياسات الجهات الرسمية التي تتعلق بالانترنت والتجارة الالكترونية تبحث عن تشجيع القطاع الخاص لقيادة هذه الانشطة ولوضع تشريعات ذات طبيعية تقنية مؤسسة على ان الانترنت اهم وسيطة اتصال وتجارة على المستوى الداخلي والخارجي .

لهذه الاسباب فان الرئاسة الامريكية مثلا أنشات فريق عمل في حقل التصرفات غير القانونية برأسة النائب العام، من اجل تقييم التشريعات الفدرالية القائمة ومدى كفايتها لتغطية التصرفات غير القانونية على شبكة الانترنت ، واستظهار الوسائل والاليات المطلوبة للجهات القانونية من اجل فعالية ملاحقة وتحري والتحقيق في مثل هذه التصرفات ، ومن اجل استخدام الوسائل التعليمية والتدريبية لتخفيف مخاطر هذه التصرفات ، واستنادا الى هذه الاهداف وضع فريق العمل استراتيجية

من ثلاثة اقسام تتعلق بالتصرفات غير القانونية ، وتوصلت الى ثلاثة خلاصات اساسية تبعا لكل قسم : -

1 – ان أي تنظيم للتصرفات غير القانونية على شبكة الانترنت يتعين ان يستند الى قاعدة اساسية وهي ضمان ان التصرفات عبر الخط تعامل بنفس الطريقة للتصرفات خارج الخط ، وبشكل يأخذ بعين الاعتبار المصالح الاجتماعية كالخصوصية وحماية الحريات المدنية .

2 - جهات تنفيذ القانون عليها ان تعي وبشكل خاص الطبيعة التقنية للانترنت وان تتدرب وتتأهل للتعامل مع مثل هذه السلوكيات ، الى جانب الحاجة الى وسائل ومقدرات تحقيق جديدة على المستوى الفدرالي والمحلي وفي ميدان التعاون الدولي لمواجهة هذه التصرفات .

3 - يتعين الاستمرار بدعم القطاع الخاص وتطوير ادواته للتنظيم الذاتي للانترنت مثل اخلاقيات عالم التكنولوجيا (CYBERETHICS) والمعايير التقنية والقواعد الاعلانية وغيرها التي من شأنها ان تعلم مستخدمي الانترنت لحماية انفسهم وعلى الاقل تقليل المخاطر من الانشطة غير القانونية .

ان التصرفات غير القانونية على وعبر شبكة الانترنت في تزايد ملحوظ ، والامثلة عليها يصعب تقصيها جميعا ، ففي 7 نيسان 1999 ارسل احد زائري مجلة اخبار مالية تدار من قبل مؤسسة ياهو رسالة بريد الكتروني تحت عنوان اخبار البيع تتضمن ان شركة PAIRGAIN قد تم شرائها من شركة (اسرائيلية) وتضمنت الرسالة مدخلا الى احد المواقع التي تعرض خدمات جديدة وتشير الى مزيد من التفاصيل حول هذا الخبر ، وبمجرد انتشار الخبر فان اسهم الشركة قد ارتفعت 30 سنتا ، ونمت عمليات التداول وازدادت بنحو 7 مرات ، لكن كان هناك مشكلة وهي ان هذا الخبر مصطنع وغير صحيح ، والموقع الذي يظهر انه يتضمن تفاصيل بشانه هو ايضا موقع وهمي ، وعندما انتشر خبر ان المعلومات السابقة غير صحيحة انخفضت اسعار الاسهم بشكل مريع، ملحقة خسائر مالية ضخمة بالعديد من المستثمرين الذين اشتروا تلك الاسهم استنادا الى الخبر الاول ، وبعد اسبوع

من هذه الواقعة تمكنت وكالة التحقيقات الفدارلية الامريكة FBI من اعتقال رجل من شمال كرولاينا ، وقد اعتبر هذا الشخص اول محتال – وطبعا لم ولن يكون الاخير - في حقل الاسهم المالية يستخدم وسيلة احتيال مواقع الانترنت ، وقد تم ملاحقة هذا الشخص من خلال عنوان الانترنت IP ، وتم اتهامه بالاحتيال عن طريق نشر معلومات مزورة حول اسهم الشركات المساهمة ، وقد اقيمت ضده ايضا دعوى مدنية للتعويض عن الاضرار التي الحقها بالمستثمرين ، وفي اب 1999 تم الحكم عليه بالسجن لمدة خمسة سنوات والزامه بدفع مبلغ 93 الف دولار .

ان الانترنت شأنها شأن غيرها من التقنيات الجديدة ، تعد قيمة اضافية للمعرفة والاداء والادارة الفاعلة في مختلف حقول النشاط الانساني وفي مقدمتها التجارة الالكترونية، ويمكن استخدامها لمزيد من الفوائد الاجتماعية والاقتصادية والسياسية والثقافية ، ولكنها تستخدم ايضا لالحاق الضرر بالمجتمع وبالقيم الاجتماعية فالتقنيات الجديدة تخلق عادة تصرفات وسلوكيات جديدة وتقدم وسائل جديدة لارتكاب الانماط الجرمية والافعال الضارة ، وهذا القول ينطبق على كل تقنية جديدة ، فالتلفون فتح الباب امام انماط جرمية جديدة (كالاحتيال عن بعد بواسطة الهاتف) اضافة الى ما قدمه من تسهيل لارتكاب الانماط الجرمية القديمة (انشطة الازعاج) . ولا تختلف الانترنت عن التقنيات الاخرى لؤلائك الذين يسعون الى ارتكاب الأفعال غير القانونية ، ففي عام 1999 على سبيل المثال، تعرضت انظمة عشرات الالوف من مستخدمي الكمبيوتر الى الاصابة بفايروس ميلسا (MELISSE) وانواع اخرى من الفيروسات التي انتشرت حول العالم عبر البريد الالكتروني والانترنت ، وادت الى الاضرار بالملفات وتدمير الانظمة والحقت بالشركات ملايين الدولارات من الخسائر ، وفي فترة لاحقة ايضا تعرضت كبرى مواقع الانترنت التجارية الى انشطة هجمات انكار الخدمة DENIAL-OF-CERVICE ATTACKS كما كانت العديد من المواقع هدفا الى انشطة PAGE-GACKING التي من شأنها ان تجعل المواقع ومحركات البحث تعمل لغير المشتركين وفي غير ما يطلب .

ان الانترنت اضافة الى ما تقدم ، مثلت ايضا وسيلة جديدة لارتكاب انشطة جرمية تقليدية بطرق اكثر تعقيدا ويسرا بالنسبة للجناه ، كما هو الحال بالنسبة للاحتيال FRAUD ، وكذلك توزيع المواد الاباحية وترويج الدعارة PORNOGRAPHY ، وبيع الاسلحة والمخدرات وغيرها من انشطة الاجرام المنظم وكذلك انشطة التوزيع غير المصرح به وغير القانوني لبرامج الحاسوب وغيره من مصنفات الملكية الفكرية ، وفي غالبية الاحوال فان انشطة الانترنت غير المشروعة تقود الى انشطة عنف مادية ، اضافة الى المخاطر التي يمكن ان يتعرض لها امن التجارة الالكترونية في ظل التزايد الرهيب في هذا الحقل ، كل ذلك يضع المشرعين والمنفذين وجهات الصناعة وجهات القانون وجهات ملاحقة الجرائم امام تحديات كبيرة .

كما اوضحنا فيما سبق وعلى نحو تفصيلي ، فان تعريف جريمة الكمبيوتر يختلف ليس فقط في حقل التقنية او القانون وانما في مختلف فروع البحث تبعا للمراد بالتعريف والغرض من استخدامه ومما استفدناه من تناول هذا الموضوع فيما سبق ان كل جريمة ترتكب بواسطة الكمبيوتر لا تكون بالضرورة جريمة كمبيوتر فعلى سبيل المثال اذا قام شخص بسرقة رمز الدخول للهاتف وبواسطته تمكن من اجراء مكالمات دولية بعيدة ، فان الرمز المسروق يجري فحصه والتعرف عليه من قبل الكمبيوتر قبل اجراء المكالمة، وبرغم ذلك فان مثل هذه الجريمة تعامل على انها احتيال وليست جريمة كمبيوتر ، وبكثير من القضايا لا يمكن تبويبها ضمن الطوائف المتعلقة بجريمة الكمبيوتر ، وقد تجد موقعها الطبيعي في جرائم الاتصالات التقليدية التي نصت عليها قوانين الاتصالات ، عوضا عن الخلاف الكبير والغير مستقر حتى الان بشأن طوائف جرائم الكمبيوتر والخلط التي قد يحصل بين جرائم تتشابه السلوكيات فيها ويمكن وصفها بذات الوصف لكن احداها جريمة كمبيوتر والاخرى ليست كذلك ، فعلى سبيل المثال فان محاسب البنك الذي يقوم بسرقة مبلغ من الصندوق يعد مختلسا ، كذلك فان محاسب البنك الذي يقوم بكتابة برنامج كمبيوتر من شأنه سرقة اجزاء النقد الصغيرة من الحسابات المختلفة

وتدويرها ونقلها الى حساب في بنك اخر عن طريق انظمة نقل الالكتروني للاموال يعد مختلسا ايضا من زاوية استيلائه على اموال بحكم ادارتها ، ومع ان كلتا الجريمتين تتصلان بالانظمة البنكية وبمعرفة نظم العمل والرقابة ، فان الثانية تعد جريمة الكمبيوتر على خلاف الاولى ، ووفقا لما سبق لنا ايضاحه حول خصائص ومحل ومتطلبات جريمة الكمبيوتر .

والكمبيوتر – كما اسلفنا ايضا – قد يلعب احد ثلاثة ادوار في الحقل الجنائي فالكمبيوتر اولا قد يكون الهدف TARGET للجريمة ، وهذا يحصل عندما يكون السلوك موجها للحصول الى المعلومات بدون تصريح ، او الحاق الضرر بالمعطيات او بنظام الكمبيوتر او شبكة الكمبيوتر ، فالفيروسات والديدان التقنية التي تطلق من قبل الهاكرز مثال على هذا النمط . والكمبيوتر ثانيا قد يكون وسيلة ارتكاب الجرم ، كما هو الحال بانشطة الاحتيال والتزوير وقد يكون الكمبيوتر ثالثا بيئة ارتكاب الجرم كما هو الحال بتخزين معلومات مروجي المخدرات كالاسماء والتواريخ والكميات لتخزن بالصورة الالكترونية بدلا من الاوراق ، وكل دور من هذه الادوار قد يكون موجودا في حالة جنائية واحدة وقد يتم استخدام الكمبيوتر لاكثر من دور في الجرم الواحد .

ومن اوضح المظاهر لاعتبار الكمبيوتر هدفا للجريمة في حقل التصرفات غير القانونية ، عندما تكون السرية CONFIDENTEALETY والتكاملية او السلامة INTEGRETY ، والقدرة او التوفر AVAILAPILITY هي التي يتم الاعتداء عليها بمعنى ان توجه هجمات الكمبيوتر الى معلومات الكمبيوتر او خدماته بقصد المساس بالسرية او المساس بالسلامة والمحتوى والتكاملية ، او تعطيل القدرة والكفاءة للانظمة للقيام باعمالها ، وهدف هذا النمط الاجرامي هو نظام الكمبيوتر وبشكل خاص المعلومات المخزنة داخله، بهدف السيطرة على النظام دون تخويل ودون ان يدفع الشخص مقابل الاستخدام (سرقة خدمات الكمبيوتر ، او وقت الكمبيوتر) او المساس بسلامة المعلومات وتعطيل القدرة لخدمات الكمبيوتر وغالبية هذه الأفعال الجرمية تتضمن ابتداءا الدخول غير المصرح به الى النظام الهدف UNAUTHORIZED

ACCESS والتي توصف بشكل شائع في هذه الايام بأنشطة الهاكرز كناية عن فعل الاختراق HACKING .

والافعال التي تتضمن سرقة للمعلومات تتخذ اشكالا عديدة معتمدة على الطبيعة التقنية للنظام محل الاعتداء ، وكذلك على الوسيلة التقنية المتبعة لتحقيق الاعتداء ، فالكمبيوترات مخازن للمعلومات الحساسة ، كالملفات المتعلقة بالحالة الجنائية والمعلومات العسكرية وخطط التسويق وغيرها ، وهذه تمثل هدفا للعديد من الجهات بما فيها ايضا جهات التحقيق الجنائي والمنظمات الارهابية وجهات المخابرات والاجهزة الامنية وغيرها ، ولا يتوقف نشاط الاختراق على الملفات والانظمة غير الحكومية ، بل يمتد الى الانظمة الخاصة التي تتضمن بيانات قيمة ، فعلى سبيل المثال قد يتوصل احد المخترقين للدخول الى نظام الحجز في احد الفنادق لسرقة ارقام بطاقات الائتمان ، وتتضمن بعض طوائف هذا النمط انشطة السرقة والاعتداء على الملكية الفكرية ، كسرقة الاسرار التجارية واعادة انتاج ونسخ المصنفات المحمية وتحديدا برامج الحاسوب . وفي حالات اخرى فان افعال الاختراق التي تستهدف انظمة المعلومات الخاصة تستهدف منافع تجارية او ارضاء اطماع شخصية كما ان الهدف في هذه الطائفة يتضمن انظمة سجلات طبية وانظمة الهاتف وسجلاته ونماذج تعبئة البيانات للمستهلكين وغيرها .

3 -6 -2 جرائم الانترنت التي تستهدف الاطفال (انشطة المواد الاباحية)

ان الاطفال والمراهقين يصبحون ضحايا لجرائم الانترنت بشكل متزايد ، ويكون ذلك في الغالب الاعم بسبب ثقتهم بالاخرين وبسبب غياب التوجيه او الرقابة في كثير من الاحيان ، ولانه لا تتوفر لديهم الخبرة والدراية الكافية لتقدير المخاطر .

وابرز انماط الجرائم التي تستهدف الاطفال عبر الانترنت تتمثل بما يلي :

1 – اقحام الاطفال باتصالات عبرالخط يكون غرضها انشطة جنسية Sexual acts.

2 – استخدام الانترنت لترويج وانتاج وتوزيع مواد دعارة الاطفال Child pornography .

3 – استخدام الانترنت لاجبار الشباب والاطفال على ممارسة افعال الدعارة وتشجيعهم لتبادلها

4 – اقحام الاطفال في انشطة سياحية تستهدف اغراض جنسية كالسفر للمشاركة في انشطة غير اخلاقية سواءا لكسب مادي او لتحقيق منافع شخصية.

5 – تنسيق وتنظيم الانشطة الجنسية الواقعية او الاتصالات الجنسية باستخدام البريد الالكتروني او التلفون او انتقال الشخص فعلا الى مكان مادي لاجراء هذه الانشطة الجنسية .

6 – توزيع المواد الجنسية غير المطلوبة اصلا ، حيث وبمجرد الاتصال بالانترنت او فتح البريد الالكتروني او الدخول على بعض المواقع المشروعة، تظهر مواد جنسية وصور خلاعية دون ان يكون الشخص قد طلبها .

7 – انشطة الابتزاز وتشويه السمعة والتهديد الموجهة للشباب والاطفال عبرالرسائل الالكترونية سواءا تتصل باغراض جنسية او جرمية او غيرها .

ان حجم مشكلة المواد الاباحية بوجه عام ، والمواد والانشطة الجنسية المتصلة بالاطفال والقصر بوجه خاص ، يتزايد بشكل غير عادي ، ووفقا لتقديرات حديثة فان واحدا من كل خمسة شباب قد توصل مع احد مواقع المواد الجنسية على الانترنت ، وان واحدا من كل ثلاثة وثلاثين شاب تلقى عرضا لانشطة جنسية بشكل او بأخر ، وان كل واحد من اربعة شباب وصلته مواد جنسية غير مطلوبة وان كل واحد من سبعة عشر شاب تلقى تهديدات او ابتزازات او غيرها من المواد المسيئة ، ذلك كله خلال عام 2000 وفقا للدراسة التي اجراها مكتب ضحايا الجريمة التابع لوزارة العدل الامريكية .

3 -6 -3 انشطة غسيل الاموال الكترونيا [1].

تعتبر جرائم غسيل الاموال الكترونيا Electronic Money Laundering من اخطر جرائم عصر الاقتصاد الرقمي ، انها التحدي الحقيقي أما مؤسسات المال للإبداع ، وهي امتحان لقدرة القواعد القانونية على تحقيق فعالية مواجهة الانشطة الجرمية ومكافحة انماطها المستجدة .

وغسيل الاموال بوجه عام ، او جريمة ذوي الياقات البيضاء ، تماما كغيرها من الجرائم الاقتصادية التي ترتكب من محترفي الاجرام الذين لا تتواءم سماتهم مع السمات الجرمية التي حددتها نظريات علم الاجرام والعقاب التقليدية .

كما ان جرائم غسيل الاموال تنشا في الغالب كجريمة لاحقة لانشطة جرمية حققت عوائد مالية غير مشروعة ، فكان لزاما اسباغ المشروعية على العائدات الجرمية او ما يعرف بالاموال القذرة ، ليتاح استخدامها بيسر وسهولة ، ولهذا تعد جريمة غسيل الاموال مخرجا لمأزق المجرمين المتمثل بصعوبة التعامل مع متحصلات جرائمهم ، خاصة تلك التي تدر اموالا باهظة ، كتجارة المخدرات وتهريب الاسلحة والرقيق وانشطة الفساد المالي ومتحصلات الاختلاس وغيرها.

وتجدر الاشارة هنا ان الذهن العام بخصوص جرائم غسيل الاموال ارتبط بجرائم المخدرات ، بل ان جهود المكافحة الدولية لغسيل الاموال جاءت ضمن جهود مكافحة المخدرات ، ولهذا نجد ان موضع النص دوليا على قواعد واحكام غسيل الاموال جاء ضمن اتفاقية الأمم المتحدة المتعلقة بمكافحة المخدرات ، ومبرر ذلك ان انشطة المخدرات هي التي اوجدت الوعاء الاكبر للاموال القذرة بفعل متحصلات عوائدها العالية ، غير ان هذه الحقيقة آخذة في التغيير ، اذ تشير الدراسات التحليلية الى ان انشطة الفساد المالي والوظيفي خاصة في الدول النامية من قبل المتنفذين والمتحكمين بمصائر الشعوب ، ادت الى خلق ثروات باهظة غير مشروعة تحتاج لتكون محلا لغسيل الاموال كي يتمكن اصحابها من التنعم بها ، وكذلك ، شهد العالم مؤخرا ما اطلق من حملات وشعارات لمكافحة الارهاب ، ارتبطت بشكل عضوي

[1] هذا العرض ايجاز شديد للموضوع مدار البحث الذي يتصل بموضوعات اخرى كالبنوك الالكترونية والاعمال الالكترونية التي نتناولها تفصيلا في الكتاب الرابع من هذه الموسوعة ، كما انه اختصار شديد لبعض المسائل التي نبحثها تفصيلا في مؤلفنا المعد للطبع قريبا باذن الله حول غسيل الاموال .

بتجفيف منابع المنظمات التي وسمت بالارهاب ، وملاحقة انشطتها الرامية لاخفاء مصادر تمويلها ، وهو ما استدعى اعادة النظر في تشريعات الارهاب نفسها او تشريعات غسيل الاموال القائمة لا في امريكا وبريطانيا وففرنسا فقط ، بل في مختلف دول العالم المتقدمة والنامية – وهو ما سيكون موضعا لدراسة تفصيلية في الوقت القريب باذن الله - ولا نبالغ ان قلنا ان شعار مكافحة الارهاب اتاح مؤخرا تحقيق تقدم كبير في انشطة مكافحة غسيل الاموال ، اذ لم تكن نفس الدول التي اطلقت هذه الحملات متحمسة الى هذا القدر لملاحقة اية انشطة غير مشروعة لتوظيف الاموال او نقلها او اسباغ مصدر مشروع عليها كبديل لمصدرها غير المشروع او المجهول .

كما اظهر التطور الحديث لجرائم الكمبيوتر والانترنت واغراض هذه الجرائم ان عائدات هذه الجرائم من الضخامة بمكان بحيث تتطلب انشطة غسيل للاموال المتحصلة منها ، خاصة ان مقترفيها في الغالب ليس لديهم منافذ الانفاق الموجودة لدى عصابات المخدرات ، وذات القول يرد بخصوص الانشطة اللاأخلاقية وتجارة الاسلحة وتجارة الرقيق والقمار ، خاصة مع شيوع استخدام الانترنت التي سهلت ادارة شبكات عالمية للانشطة الاباحية وانشطة القمار غير الشرعية .

وغسيل الاموال ايضا ، نشاط اجرامي تعاوني ، تتلاقى فيه الجهود الشريرة لخبراء المال والمصارف ، وخبراء التقنية - في حالات غسيل الاموال بالطرق الالكترونية - وجهود خبراء الاستثمار المالي ، الى جانب جهود غير الخبراء من المجرمين ، ولهذا تطلبت مثل هذه الجرائم دراية ومعرفة لمرتكبيها ، ولهذا تطلبت عملا وتعاونا يتجاوز الحدود الجغرافية ، مما جعلها جريمة منظمة تقارفها منظمات جرمية متخصصة وجريمة عابرة للحدود ذات سمات عالمية ، ومن هنا يتعزز القول بانه ليس من السهل مكافحتها دون جهد دولي وتعاون شامل يحقق فعالية انشطة المكافحة .

لا احد يعرف الحجم الحقيقي للمبالغ التي يجري غسلها عبر انشطة غسيل الاموال الجرمية ، ولكن ثمة اتفاق عالمي انها مبالغ ضخمة بالمليارات ، والتقدير الحالي انها تصل نحو 500 بليون في العالم ، وجرائم غسيل الاموال ليست حكرا

على الدول الصناعية او مجتمعات الثروة ، بل انها تتسع وتنمو في بنية الدول التي يسهل النفاذ عبر ثغرات نظامها القانوني.

وبالرغم من ان اشكال وانماط ووسائل غسيل الاموال متغيرة وعديدة ، وثمة اتجاه عريض لتحويل الاموال القذرة الى اصول مالية (مواد ثمينة) ، وموجودات عقارية او نحو ذلك ، فان البيئة المصرفية تظل الموضع الاكثر استهدافا لانجاز انشطة غسيل الاموال من خلالها ، واذا كانت البنوك مخزن المال ، فانه من الطبيعي ان توجه انشطة غاسلي الاموال القذرة الى البنوك على امل اجراء سلسلة من عمليات مصرفية تكتسي بنتيجتها الاموال القذرة صفة المشروعية .

ولهذا تعد البنوك المستهدف الرئيسي في عمليات غسيل الاموال ، ويرجع ذلك الى دور البنوك المتعاظم في تقديم مختلف الخدمات المصرفية وتحديدا عمليات الصرف والتحويل النقدي بواسطة الشيكات والشيكات السياحية (الاجنبية) والحوالات المالية خاصة بالوسائل الالكترونية وبطاقات الائتمان والوفاء وعمليات المقاصة وادارة المحافظ الاستثمارية وتداول العملات والاسهم وغيرها ، وهذه الخدمات يتسع مداها ونطاقها في عصر المعلومات وتتحول الى انماط اكثر سهولة من حيث الاداء واقل رقابة من حيث آلية التنفيذ ، خاصة في ميدان البنوك الالكترونية او بنوك الويب على شبكة الانترنت ، ومثل هذه العمليات بشكليها التقليدي والالكتروني خير وسيلة لتستغل بغرض من اجل اخفاء المصدر غير المشروع للمال .

ومن جهة اخرى ، فان البنوك ذاتها ، تعد راس الحربة في مكافحة انشطة غسيل الاموال ، لحماية نفسها أولا من المخاطر المالية والمسؤوليات القانونية المترتبة على خوضها او مشاركتها في هكذا انشطة ، وللمشاركة الفاعلة في الجهد الدولي لمكافحة جرائم غسيل الاموال .

وتحتاج البنوك لمعرفة معمقة وشاملة بشان الاليات التي تتبع لغسيل الاموال مع الادراك انها اليات متغيرة ومعقدة غالبا ما تنشا من فكرة احتيالية او جرمية تولدت عن معرفة معمقة لصاحبها بالعمل المصرفي ، ان لم يكن قد لجا لخبرة مصرفية مميزة للحصول على الفكرة . من هنا كانت عمليات غسيل الاموال

في الحقل المصرفي وليدة (خبرة) مصرفية ، ومن هنا ايضا فان كشفها ومنعها يحتاج (خبرة) مصرفية ، وهذا ما يدفعنا للقول ان غسيل الاموال ومكافحته صراع بين خبرات فنية من ذات المصدر والبيئة مع تباين في الهدف ، فغسيل الاموال جهد شرير ومكافحته جهد خير ، وبين الخير والشر ثمة مساحة من الاجتهاد والحركة يجب ان تسد دائما لصالح الخبرة الخيرة اذا ما اريد لانشطة المكافحة ان تنجح وتحقق فعالية مميزة .

وحتى وقت قريب كان يسود الاعتقاد ان يد القضاء لا تمتد الى الاشخاص الاجانب الذين يملكون المال القذر او يمارسون انشطة تتصل بغسيل الاموال من خارج الحدود او اؤلئك الذين لا ينتسبون الى نطاق اختصاص المحكمة التي يوجد في نطاقها المؤسسة المصرفية او المالية التي تم من خلالها اجراء عمليات الغسل وكذلك كان يسود الاعتقاد ان مكافحة غسيل الاموال مقتصر على اموال المخدرات القذرة ، وبكل الحالات لا يمتد الى الاموال الناشئة عن الفساد المالي والاداري للقيادات والمسؤولين المدنيين والعسكريين ، لكن هذا المفهوم يتغير شيئا فشيئا ، وتمتد يد القضاء لتطال من هم خارج نطاق الاختصاص المكاني للمحاكم ولتطال ايضا مسؤولين متنفذين عن محاولات وانشطة غسيل الاموال المتحصل من الفساد الاداري وتمثل قضية لوزارينكو (رئيس الوزراء الاوكراني السابق) مثالا مميزا في هذا الحقل فقد تمت ادانته بانشطة غسيل الاموال من قبل القضاء السويسري ، وفي الوقت ذاته وبعد هربه الى امريكا ومحاولاته اللجوء السياسي للتملص من الحكم السويسري الصادر بحقه ، جرى توجيه الاتهامات اليه وتجري محاكمته امام القضاء الامريكي .

وكان قد ادين لوزارينكو من قبل القضاء السويسري بتاريخ 2000/6/29 بالحبس لمدة 18 شهرا لقيامه بانشطة غسيل اموال تبلغ 880 مليون دولار في الفترة ما بين 94 - 97 ، من بينها 170 مليون تم غسيلها عبر حسابات سويسرية ، أما لوزارينكو فقد اعترف بعملية غسل 9 ملايين فقط ، وقد تم اعتقال لوزارينكو من قبل السلطات السويسرية في كانون الثاني عام 1998 عندما دخل سويسرا بجواز سفر بنمي (بنما) مزور ، واطلق سراحه بالكفالة البالغة 3 ميلون دولار امريكي ، وما لبث ان غادر

الى الولايات المتحدة في عملية لجوء سياسي في نيسان عام 1990 ، بعد ان تم ضبطه من قبل دائرة الهجرة في نيويورك لخرقه نظام الهجرة والفيزا ودخوله غير المشروع وبناء على طلب امريكي، قامت السلطات السويسرية بتجميد ارصدة 20 حساب بنكي يعتقد انها تعود الى لوزارينكو ، وتم القاء القبض عليه واحتجازه ومنع كفالته نيابة عن السلطات السويسرية ، ولم يلبث ان تقدم المدعي العام في سان فرانسيسكو بلائحة اتهام ضد لوزارينكو وشخص اخر هو بيتر كيرتشينكو الذي يعتقد بانه هو الذي قام بتنفيذ عمليات غسيل الاموال ، وتتضمن اللائحة اتهامهما بتحويل 114 مليون دولار امريكي الى (البنك التجاري في سان فرانسيسكو ، والباسفيك بنك ، ووست اميركا بنك ، وبنك اوف اميركا ، وميرل لينش ، ولمؤسسة افليت بوستن روبيرتسون) خلال الاعوام من 94 -99 ، ولم يتم توجيه الاتهام الى أي من هذه المؤسسات ، اضافة الى توجيه الاتهام لهما بشراء موجودات ومشاريع في امريكا خلال عامي 97 - 98 نقدا . وتوجيه الاتهام بالاحتيال وتحويل اموال مسروقة الى الولايات المتحدة ، وقد اجاب لوزارينكو في الجلسة الافتتاحية بتاريخ 13 حزيران 2000 بانه غير مذنب .

وقد نشات هذه القضية جراء انشطة تحقيق امتدت الى عامين كاملين تعاونت فيها الشرطة الفدرالية الامريكية واجهزة التحقيق في سويسرا اضافة الى جهات امنية في روسيا الاتحادية واوكرانيا ، وجرى التحقيق في مصادر هذه الاموال التي تبين انها نجمت عن استغلال رئيس الوزراء لمهام وظيفته هذه التي تولاها في الفترة ما بين ايار 96 وحتى تموز 97 ، وجراء تلقيه مبالغ نقدية من افراد ومؤسسات ورشاوى لتسهيل تنفيذهم لاعمالهم ، وتعد هذه القضية اول قضية وفق قانون غسيل الاموال الامريكي تستخدم الاجراءات فيها بشأن انشطة ارتكبت خارج الولايات المتحدة وتتعلق بشخص من خارجها ، وتستند المحكمة في اختصاصها الى ان جزءا من الانشطة الجرمية في بعض الحالات قد ارتكب داخل الولايات المتحدة ، وجزءا اخر من الانشطة كانت الولايات المتحدة فيه محطة لعمليات التحويل وادماج المبالغ محل الجريمة ضمن

النظام المالي الامريكي واعادة تحويلها الى جهات اجنبية اخرى ، الى جانب ايداع النقود في بنوك الولايات المتحدة وشراء موجودات ومشروعات فيها .

وجريمة غسيل الاموال لا تقف عند حد امتلاك شخص لمال غير مشروع وادخاله في النظام المالي للدولة ، بل هذا مفهومها البسيط ، وهي في الحقيقة جريمة تتعدد انماطها وتطال المسؤولية فيها مرتكبها والمساهمين فيها والمتدخلين والمنتفعين ، ولعل الوقوف على انماط جرائم غسيل الاموال يستدعي ابتداءا تحديد المقصود بغسيل الاموال من الوجهة القانونية وتبين مراحل تنفيذها .

ويعد تعريف دليل اللجنة الاوروبية لغسيل الاموال الصادر لعام 1990 الاكثر شمولا وتحديدا لعناصر غسيل الاموال من بين التعريفات الاخرى التي تضمنتها عدد من الوثائق الدولية والتشريعات الوطنية ، ووفقا للدليل المذكور فان غسيل الاموال ((عملية تحويل الاموال المتحصلة من انشطة جرمية بهدف اخفاء او انكار المصدر غير الشرعي والمحظور لهذه الاموال او مساعدة أي شخص ارتكب جرما ليتجنب المسؤولية القانونية عن الاحتفاظ بمتحصلات هذا الجرم)) وعملية الاخفاء او الانكار تمتد لحقيقة او مصدر او موقع او حركة او ترتيبات او طبيعة الحقوق المتحصلة من هذه الاموال او ملكيتها مع توفر العلم ان هذه الاموال متحصلة من جريمة جنائية ، ووفقا لهذا التعريف فان غسيل الاموال بالمعنى البسيط هو اظهار المال الناتج عن جرائم جنائية - كترويج المخدرات او الارهاب او الفساد او غيرها - بصورة اموال لها مصدر قانوني ومشروع .

هذا عن المفهوم ، أما عن كيفية تحقق غسيل الاموال ، او مراحل ذلك ، فلا بد لنا ان نتذكر ان عملية غسيل الاموال ليست فعلا واحدا ، ولكنها عملية تنطوي على مراحل وسلسلة من الاجراءات من هنا يكون لادراك مراحلها اهمية في تحديد ما ينشأ من صور جرمية ترتبط بهذه المراحل ، وبشكل عام فان غسيل الاموال يمر بمراحل اساسية ثلاث ، يمكن ان تحصل جميعها دفعة واحدة ويمكن ان تحصل كل مرحلة فيها مستقلة عن الاخرى او الواحدة تلو الاخرى ، فالمرحلة الاولى هي عملية ادخال المال في النظام المالي القانوني PLACEMENT ، وهدف هذه

المرحلة التخلص من كمية النقد الكبيرة بين يدي مالكها في البلد او الموضع الموجودة فيه ، وذلك بنقلها من موضعها او موضع الحيازة وتحويلها الى اشكال نقدية او مالية مختلفة كالشيكات السياحية والحوالات البريدية وغيرها . أما المرحلة الثانية فهي عملية نقل وتبادل المال القذر ضمن النظام المالي الذي تم ادخالها فيه ALYERING . واما المرحلة الثالثة فتتمثل بعملية دمج المال نهائيا بالاموال المشروعة لضمان اخفاء المصدر القذر لها INTEGRATION ، ولتحقيق نجاح هذه العمليات الثلاث فان استراتيجيات غسيل الاموال الجرمية تنطلق من الحاجة الى اخفاء المصدر الحقيقي للملكية غير المشروعة ، والحاجة الى المحافظة على ترتيبات عملية غسيل الاموال ، والحاجة الى تغيير الالية وتعددها من اجل تحصيل كمية كبيرة من النقد المشروع .

اذا ، امام التعريف المتقدم ، وامام مراحل عملية غسيل الاموال المتقدمة ، يمكننا تبين الانماط الجرمية الرئيسية التالية لعمليات غسيل الاموال : -

1 - جريمة غسيل الاموال نفسها باعتبارها الجريمة الاساسية التي تنشأ عن امتلاك شخص (طبيعي او معنوي) اموالا غير مشروعة جراء جريمة جنائية اخرى ، واتجاه نية هذا الشخص لمباشرة عمليات غسلها وابرام الاتفاق لتفيذ ذلك مع الجهات الوسيطة والمنفذة والمساهمة .

2 - جريمة المساعدة في انشطة غسيل الاموال مع توفر العلم بان المال غير مشروع ، وتمتد هذه الجريمة الى كل من ساهم في اية ترتيبات او اجراءات في اية من مراحل غسيل الاموال المشار اليها اعلاه سواء اكان شخصا طبيعيا او معنويا ، وهي الصورة الجرمية التي يجري على اساسها ملاحقة المؤسسات المالية والمصرفية اذا ما كانت متورطة في ترتيبات او اجراءات غسيل الاموال وهي جريمة قصدية يتطلب لها من حيث الركن المادي توفر العلم لدى مرتكبها بعدم مشروعية المال واتجاه ارادته لتنفيذ النشاط الجرمي الذي يتبع في صورته المرحلة التي يساهم فيها .

3 - حيازة او امتلاك او الاحتفاظ بالاموال محل عملية الغسيل او متحصلاتها مع العلم بالطبيعة غير المشروعة لها ، والفرض في هذه الصورة ان الشخص ليس

متورطا بعمليات الغسيل ذاتها وانما يحتفظ او يحوز او يتملك المال غير المشروع على نحو يساهم في اخفاء مصدر المال، ويساعد المجرم الذي يملك المال اصلا في الاحتفاظ بمتحصلات الجريمة ، وهي ايضا جريمة قصدية تتطلب صورة القصد في ركنها المعنوي .

4 - جريمة عدم الابلاغ عن انشطة غسيل الاموال المشبوهة ، او الاخفاق في منعها او الاهمال في كشفها ، او مخالفة متطلبات الابلاغ عنها ، او الاخلال بالتزامات الابلاغ عن الانشطة المصرفية او المالية المقررة بموجب تقارير الرقابة الداخلية او الخارجية وتقارير المؤسسات ذات العلاقة عند توفر الرابط بينها وبين المؤسسة المعنية ، وهذه الصور اضافة الى صور فرعية تنشأ عنها ، تتعلق بجرائم في غالبها ليست قصدية وانما من قبيل جرائم الخطأ والاهمال ، لكنها تنشأ مسؤوليات جزائية ومدنية وتأديبية ايضا، وهي التزامات تتصل بالتعليمات والانظمة المقررة في المؤسسات المالية والرقابية او التي تتقرر بموجب القوانين كما في العديد من الدول الاوروبية وامريكا .

هذه هي ابرز الصور الجرمية في ميدان غسيل الاموال ، وتتباين الاتجاهات التشريعية الوطنية بشأنها ، فنجد على سبيل المثال القوانين البريطانية تحدد خمسة انماط من بين جرائم غسيل الاموال في حين نجدها اوسع من ذلك في القانون الامريكي لما يتضمنه من تفصيلات بشأن الادوار الوسيطة والنهائية للمساهمين في عمليات غسيل الاموال ، ولكن بالعموم ، فان الاطار العام لتجريم انشطة غسل الاموال ينطلق من محاور اساسية ، اولها وجود الاموال القذرة ، وهي هنا اموال متحصلة من جرائم جنائية تفتقد لاي مصدر من مصادر اكتساب الاموال المشروعة وثانيها : القيام بسلوكيات مادية تستهدف اخفاء المصدر غير المشروع لهذه الاموال وهذه السلوكيات تتباين تبعا لدور مرتكبها في عملية غسيل الاموال وتتباين ايضا بين سلوكيات ايجابية ، أي القيام بعمل، وسلوكيات سلبية أي الامتناع عن العمل . وثالثها: توفر الركن المعنوي للجريمة الذي يتخذ في بعض صورها صورة القصد وفي صور اخرى صورة الخطأ .

واذا كانت الانماط التقليدية لغسيل الاموال فيما سبق ، اعتمدت على ادوات العمل المصرفي لادماج المال غير المشروع في النظام المالي المشروع ، فانه من الطبيعي ان تتجه انشطة غسيل الاموال الى الوسائل الالكترونية في ظل تنامي وسائل اتمتة الخدمات والاعمال المصرفية ، وفي ظل ممارسة انماط شمولية من الخدمات المالية الالكترونية ، كخدمات البنوك الالكترونية وبنوك الويب وعمليات الدفع النقدي الالكتروني ، وفي ظل تنامي الاعتماد على المال الرقمي واحلاله بديلا عن المال الورقي وشيوع البطاقات المالية بانواعها ووصولها في المرحلة الحالية الى البطاقات والمحافظ الماهرة التي يجري فيها تخزين القيم النقدية عن طريق شرائح الكترونية يعاد شحنها بالقيم والعملات المطلوبة .

ان الغسيل الالكتروني للاموال استثمار لادوات العمل المالي الالكترونية ، ولهذا فان كل وسيلة من وسائل اتمتة الخدمات والاعمال المصرفية ، تثير تحديات لدى استغلالها في انشطة غسيل الاموال غير المشروعة .

فعمليات الدفع النقدي عبر الانترنت بواسطة بطاقات الائتمان اتاحت الحصول على منتجات وخدمات يجري الوفاء بمقابلها بعيدا عن ادوات الوفاء التقليدية وبشكل قد لا يتيح رقابتها كما هو الحال في عالم العمل المصرفي التقليدي كما ان عمليات الاقتراض عبر الانترنت وتقديم الضمانات عبرها ايضا ، وعمليات فتح الحسابات لدى البنوك الافتراضية – التي لا وجود حقيقي لها في على خارطة المكان – وبعيدا عن سلطات الرقابة المصرفية والاختصاص القضائي ، تتيح احداث مراكز مالية يصار لاحقا لاستغلالها في عميلة اخفاء مصدر الاموال لتظهر بالنتيجة ان لها مصدرا مشروعا .

ولو وقفنا امام حقيقة ان العمل المصرفي والنقدي الالكتروني يمارس الان عبر الانترنت من جهات غير مصرفية اصلا ، وهو ليس مجرد حالات محدودة ، فالاعمال الالكترونية المالية والخدمات الالكترونية المالية عبر الانترنت تمارس واقعيا في حجمها الاكبر من خلال منصات ومواقع للتسويق اكثر مما تمارس من قبل البنوك ، وهذه الحقيقة تؤدي الى نتيجة هامة ، وهي ان نطاق الرقابة على هذه

الانشطة من جهات الاشراف المصرفي – كالبنوك المركزية – ليست قائمة بالنسبة لهذه الشركات باعتبارها اصلا ليست مصارف بالمعنى القانوني ، وبالتالي يسهل ان تتم عبرها انشطة غسيل الاموال ، بل علينا ان نتذكر ان اهم انشطة غسيل الاموال انشاء المشروعات الوهمية او المشروعات التي تستغل كواجهة لاخفاء مصدر المال ، وليس كالانترنت بيئة مناسبة لانشاء مثل هذه المشاريع ، اذ يكفي مثلا انشاء موقع لتسويق منتجات معينة او تقديم خدمات معينة لقاء دفعات نقدية ببطاقات الائتمان ، وبنفس الوقت اجراء عمليات شراء ودفع وهمية تؤدي في نتيجتها بان تضخ اموال في حساب الموقع لدى المصرف الذي يتولى عمليات المقاصة وادارة الدفع على الموقع ، فتستغل لاحقا باعتبار مصدرها البنك الذي يدير حساب الموقع ويتلقى ايراداته ، وفي الحقيقة فان مصدرها هي الاموال القذرة اصلا . وهذا واحد من عشرات الامثلة التقليدية او الحالات المتصورة لاستغلال البيئة الالكترونية في غسيل الاموال .

كما ان استثمار الانترنت في عمليات ادارة الاسهم والمضاربة بالعملات ومزادات البيع والشراء والمسابقات المصطنعة - واحيانا الحقيقة - وما يمنح فيها من مبالغ باهظة للفائزين بيئة خصبة لادماج الاموال القذرة في انشطة تبدو في ظاهرها انشطة مشروعة تسبغ وصفها هذا على الاموال المتحصلة منها .

ان الحاجة اصبحت ماسة لادراك آثار واوجه استخدام كل وسيلة جديدة مما يجري توظيفه في اطار سياسات توظيف التكنولوجيا ، ولا يتعين ان يقتصر هذا الادراك على الجوانب الايجابية والعملية ، بل يتعين فهم وتصور ما يمكن ان يكون استغلالا غير مشروع لهذه الوسائل .

الاستراتيجيات المصرفية والقانونية لمكافحة انشطة غسيل الاموال

ان القراءات النظرية لعشرات التقارير الدولية ، ومتابعة وسائل غسيل الاموال التي تعرضها الادلة التوجيهية ، تقدم المتطلب الاساسي للمعرفة بمخاطر هذا النشاط والياته ، لكنها قطعا لا تمثل الوسيلة الفاعلة لمكافحة هذه الانشطة . فالمعرفة متطلب رئيسي ، ومصادره متوفرة للبنوك ، لكن غير المتوفر امتحان هذه

المعرفة عمليا ، مع ان الخطورة تكمن في عدم تعميم البنوك أدلة المكافحة التوجيهية على كافة موظفيها وانحصارها في فئة الادارة العليا . وهو مسلك خاطيء لان اكبر عمليات غسيل الاموال كشفت في الغالب من قبل موظفين حاذقين لاحظوا انشطة مريبة سواء على الزبائن او اشخاص في ادارات المصرف .

والامتحان العملي لقدرة المصرف على الاحاطة بانشطة الغسيل ، يتاتى من اخضاع الموظفين الى برامج تدريبية عملية تتناول تحليلا معمقا لحالات تتصل بانشطة دوائر البنك المختلفة ، وهي حالات أما واقعية او افتراضية لكنها بالنتيجة حالات يمتحن فيها قدرة الموظف على التقاط ما يسمى (الحالة المريبة) وقدرته - سواء هو او جهة الاختصاص في البنك - على تحليل هذه الحالة والتوثق من مدى حصول النشاط غير المشروع .

في احدى الانشطة التدريبية المهمة لحالات غسيل الاموال ، لفت انتباه احد المشاركين - وهو موظف برازيلي - وجود حالة شبيهة في المصرف الذي يعمل فيه وما ان عاد الى عمله حتى شرع في تقصي الحالة ، وقدم بشانها - بعد جهد رقابي وتحليلي امتد لايام - تقريرا لادارة البنك ، وجرى اعطاءه الصلاحية للتعاون مع الجهة الرقابية للتوثق من نتائج التقصي ، وكانت مفاجاة للجميع ان يكشف جهد هذا الموظف عن محاولة للشروع في واحدة من اكبر عمليات غسيل الاموال احد اطرافها كبار المتنفذين من سياسي العالم الثالث ، الذي سعى لاسباغ المشروعية على اموال تحصل عليها من انشطة الفساد واستغلال الوظيفة . ان ما قام به هذا الموظف كان احد اهم العوامل لانشاء وحدة متخصصة في البنك لتحليل دراسة تقارير العمل ونماذج الرقابة المالية ودراسة تحليل تقارير النقد الاجنبي ونشاط الاشخاص غير المقيمين بشكل رئيس.

واما في حقل بناء اطار قانوني عربي لمكافحة جرائم غسيل الاموال ، فلا بد ابتداء من التاكيد على وجوب ان يكون هذا الاطار واضح المعالم متسما بالشمولية والاحاطة يتحقق من خلاله فعالية المكافحة وسلامة النتائج .

ويتعين ان ينطلق هذا الاطار من استراتيجية واضحة المعالم تحدد مصادر الخطر وانماط عمليات الغسيل ، والمراحل التنفيذية لها ، والترتيبات التي يتخذها غاسلوا الاموال ومعاونيهم ، والبناء القانوني القائم بما يحتويه من ثغرات تمكن غاسلي الاموال من النفاذ عبرها لتحقيق انشطتهم غير المشروعة . فاذا ما وقفنا على المحتوى الفني لعلميات الغسيل والواقع القانوني القائم الذي يتيح النفاذ انتقلنا الى تبين خصائص النظام المالي العربي والانشطة المصرفية العربية والواقع القانوني المتصل بها لتبين اوجه التخصيص المتعلقة بالبيئة العربية ، ويتكامل هاتين الصورتين تتضح لنا النتائج فتتحدد امامنا وبشكل دقيق الصور الجرمية المتعين اتخاذ التدابير لمكافحتها ، فيجري عندئذ تحديدها بشكل دقيق ، لننتقل الى الجزء الثاني من الاستراتيجية وهو آليات المكافحة ، وهي هنا اليات مركبة ادارية ومالية وقانونية يستتبعها اليات تعاون وطني واقليمي ودولي ، تترابط حلقاته وتتشابك محققة في الوقت ذاته توازنا بين اهمية المكافحة وفعاليتها من جهة ، وموجبات حماية السيادة الوطنية والاقتصاد الوطني من جهة اخرى .

وبناء هكذا استراتيجية يتعين ان يعتمد على خبرات وكفاءات بحثية وعلمية وعملية من مختلف القطاعات تحقق القدرة على الاحاطة بمختلف ابعاد المسألة القانونية والفنية والادارية ، وهو اطار يتعين ان يجيد معرفة الواقع ويتميز بسعة الاطلاع على عالم ما وراء الحدود ، فيستفيد من الانشطة المتخذة في دول اخرى وفي النظم المقارنة دون ان يغفل الخصائص الذاتية للمجتمع المحلي والاطار الاقليمي الذي تتبع له الدولة .

فاذا تحقق وجود مثل هذه الاستراتيجية كان من الواجب ان ننتقل الى اليات تنفيذها ، وهو ما يستتبع استثمار كل جهد او اطار وطني وعربي وعالمي ، وتنفيذ الاستراتيجيات يتحقق باتخاذ التدابير التشريعية (القوانين او الانظمة او التعليمات) وابرام اتفاقيات التعاون الثنائية والاقليمية والدولية ، وتنفيذ برامج التوعية العامة وتنفيذ برامج التأهيل والتدريب للاشخاص والجهات التي تنيط بها الاستراتيجية مهمة المكافحة او الرقابة على الانشطة المالية او مهمة الاخبار عن الانشطة المشكوك

بها ، ويمثل الاطار التدريبي والتأهيلي احد اهم روافع فعالية انشطة المكافحة ، فلا قيمة للتدليل الارشادي النظري او للاستراتيجية المفرغة على الاوراق او للقوانين المحفوظة بين دفتي كتاب اذا لم يتحقق للمرتبطين بها قدرة التنفيذ العملي لمحتواها ، ويتعين ان يمتد التدريب الى موظفي المؤسسات المالية والمصرفية بمختلف مراتبهم ووظائفهم والى جهات الضابطة العدلية والقضاء والقانون والى الجهات الحكومية وجهات القطاع الخاص في آن معا .

الفصل الخامس

مراجعة الحسابات في ظل التشغيل الإلكتروني للبيانات

الفصل الخامس

مراجعة الحسابات في ظل التشغيل الإلكتروني للبيانات

لقد أصبح استخدام الحاسبات الآلية في المنشآت في المملكة العربية السعودية حقيقة ملموسة لا تحتاج إلى برهان، وهذا الاستخدام أخذ في الازدياد والتطور والتوسع. وقد أثر استخدام الحاسبات الآلية في معالجة البيانات المحاسبية في عمل المراجع من ناحيتين:

الناحية الأولى: تطوير أساليب الرقابة الداخلية: فقد ترتب على استخدام الحاسبات الآلية في معالجة البيانات المحاسبية أن قامت إدارة المنشآت المختلفة بتطوير أساليب الرقابة الداخلية التي كانت قائمة في ظل نظام التشغيل اليدوي للبيانات حيث أصبحت فعالية الأنظمة التقليدية للرقابة الداخلية محل تساؤل عند تطبيق نظم التشغيل الإلكتروني للبيانات.

الناحية الثانية: أساليب المراجعة التي يعتمد عليها المراجع الخارجي: فالأساليب الفنية وإجراءات المراجعة التي كان يعتمد عليها المراجع الخارجي لتجميع الأدلة والقرائن في ظل النظم التقليدية لتشغيل البيانات المحاسبية أصبحت غير مناسبة في ظل استخدام الحاسب الآلي في تشغيل البيانات المحاسبية.

لذلك كان لابد من ظهور أساليب جديدة للمراجعة تتناسب مع التحديات التي صاحبت استخدام الحاسبات الآلية في تشغيل البيانات المحاسبية مثل:

-اختفاء السجلات المادية في بعض الأحيان.

-عدم وجود مسار واضح للمراجعة بحيث يمكن تتبع العمليات من بدايتها إلى نهايتها لبعض العمليات.

-سهولة التلاعب في الحسابات وصعوبة الاكتشاف.

ولذلك ظهرت عدة أساليب لمراجعة الحسابات المعدة باستخدام الحاسب الآلي مثل:

1 -أسلوب المراجعة حول الحاسب.

2 -أسلوب المراجعة من خلال الحاسب.

3 -أسلوب المراجعة باستخدام الحاسب.

أولاً: الملامح الرئيسية لمعيار المراجعة في المنشآت التي تستخدم الحاسب الآلي:

وفقاً لما ورد في نص معيار المراجعة في المنشآت التي تستخدم الحاسب الآلي نحدد الملامح الرئيسية للمعيار على النحو التالي:

1.يجب على المراجع الخارجي أن يفهم خصائص بيئة معالجة البيانات إلكترونياً ويأخذها بالاعتبار، لأنها:

✓تؤثر على تصميم النظام المحاسبي وما يرتبط به من رقابة داخلية،

✓تؤثر على اختبار نظام الرقابة الداخلية التي ينوى الاعتماد عليه،

✓تؤثر على طبيعة وتوقيت ومدى إجراءات عملية المراجعة.

2.لا تختلف أهداف المراجع الخارجي سواء تم معالجة البيانات المحاسبية يدوياً أو بالحاسب الآلي. ولكن قد تتأثر طرق تطبيق إجراءات المراجعة للحصول على أدلة الإثبات بالطريقة المتبعة في معالجة البيانات.

3.عند تخطيط عملية المراجعة يجب على المراجع أن يأخذ في الاعتبار الطرق المتبعة من قبل المنشأة في معالجة البيانات المحاسبية، بما في ذلك استخدام المنشأة لمؤسسات الخدمات مثل مركز الخدمة الخارجية.

4.على المراجع الخارجي عند تقييمه لتأثير معالجة المنشأة لبياناتها بالحاسب الآلي على فحص القوائم المالية أن يأخذ في الاعتبار ما يلي:

✓تحديد نطاق استخدام الحاسب الآلي في معالجة التطبيقات المحاسبية المرتبطة بالمعلومات المحاسبية التي تؤثر على القوائم المالية موضوع المراجعة.

✓نطاق الصعوبات في تشغيل الحاسب الآلي سواء كان لدى المنشأة أو لدى مركز خدمات خارجي.

✓أهمية أنظمة الحاسب الآلي في إدارة ورقابة الأعمال.

✓الهيكل التنظيمي لأنشطة معالجة البيانات بواسطة الحاسب الآلي.

✓أجهزة وبرامج الحاسب الآلي المستخدمة بواسطة المنشأة.

✓البيانات والوثائق التي يمكن أن تستخدم لإدخال البيانات في الحاسب الآلي قد تظهر فقط لفترة قصيرة من الزمن أو فقط بشكل مقروء للآلة. وفي بعض أنظمة الحاسب الآلي الأخرى لا تظهر مستندات الإدخال على الإطلاق، وذلك بسبب إدخال البيانات على الحاسب الآلي مباشرة. وقد تتطلب السياسات المستخدمة بواسطة المنشأة في تخزين بعض البيانات أو المعلومات المستخدمة في فحص أو تنفيذ إجراءات المراجعة في الوقت الذي تكون فيه هذه البيانات متاحة. بالإضافة إلى ذلك هناك بعض المعلومات الخاصة المنتجة بالحاسب الآلي للاستخدام الداخلي بواسطة الإدارة يمكن أن تكون مفيدة في تنفيذ بعض الاختبارات الأساسية للمراجع الخارجي (وخاصة إجراءات الفحص التحليلية).

✓استخدام طرق المراجعة بمساعدة الحاسب الآلي لزيادة فعالية تنفيذ إجراءات المراجعة.

5.يجب أن يأخذ المراجع الخارجي في الاعتبار ما إذا كانت هناك مهارات متخصصة يحتاجها لدراسة أثر معالجة البيانات بالحاسب الآلي على عمليات المراجعة لفهم تتابع العمليات، ولفهم طبيعة إجراءات المهارات المتخصصة يجب على المراجع أن يبحث عن مساعدة المهنيين الذين لديهم هذه المهارات، سواء من بين العاملين معه أو من غيرهم.

6.يجب أن يحصل مراجع الحسابات على تأكيدات من الإجراءات التحليلية مبنية على اتساق المبالغ المسجلة مع التوقعات التي تم الحصول عليها والمستخرجة من مصادر أخرى. ويجب أن تكون الثقة في البيانات التي استخدمت في إعداد التوقعات

كافية لدرجة التأكيد المرغوب فيها والتي تم الحصول عليها من الإجراءات التحليلية.

7.يجب على المراجع الخارجي عند تقييم المخاطر في المراحل المبدئية اكتساب معرفة كافية بالنظام المحاسبي حتى يستطيع فهم البيئة الشاملة للرقابة وفهم تدفق سير العمليات.

8.تمثل بيئة الرقابة التأثير الشامل لعوامل مختلفة في تكوين، وتعزيز أو تخفيض كفاءة سياسات وإجراءات معينة. وعلى المراجع الخارجي أن يأخذ في الاعتبار إدارة معالجة البيانات إلكترونياً عند فحص العناصر التالية:

✓الهيكل التنظيمي للمنشأة.

✓طرق تفويض الصلاحيات والمسئوليات.

✓طرق الرقابة الإدارية.

9.ينبغي على المراجع الخارجي عندما يقرر الاعتماد على الرقابة الداخلية في تنفيذ عملية المراجعة الالتزام بما يلي:

✓تحديد إجراءات وسياسات هيكل الرقابة الداخلية المناسبة للتأكيدات المحددة والتي من المحتمل أن تمنع أو تكشف الأخطاء المادية في هذه التأكيدات.

✓يقوم بإجراء اختبارات للرقابة لتقييم كفاءة هذه الإجراءات وهذه السياسات.

✓لتحديد الرقابة وتنفيذ اختبارات هذه الرقابة، يجب على المراجع الخارجي أن يأخذ في الاعتبار الرقابة اليدوية والرقابة بالحاسب الآلي والتي تؤثر على مهمة معالجة البيانات إلكترونياً (الرقابة العامة لمعالجة البيانات إلكترونياً) وكذلك الرقابة المحددة على التطبيقات المحاسبية ذات العلاقة (الرقابة التطبيقية لمعالجة البيانات إلكترونياً).

✓تهدف الرقابة العامة لمعالجة البيانات إلكترونياً إلى وضع إطار للرقابة العامة على أنشطة معالجة البيانات إلكترونياً، ولتوفير مستوى معقول من التأكد بأن الأهداف الشاملة للرقابة الداخلية قد تحققت.

10. تهدف الرقابة التطبيقية لمعالجة البيانات إلكترونياً إلى وضع إجراءات للرقابة المحددة على التطبيقات المحاسبية من أجل توفير تأكيد معقول بأن جميع العمليات مصرح بها وصحيحة ومسجلة، وتمت معالجتها على الوجه الأكمل وفي الوقت المناسب.

11. قد يكون للرقابة العامة لمعالجة البيانات إلكترونياً أثر شامل على معالجة العمليات في نظم التطبيقات. وإذا كانت هذه الرقابة غير فعالة، فقد يكون هناك مخاطر من أمكانية حدوث أخطاء دون اكتشافها في نظم التطبيقات. وبالتالي فإن نقاط الضعف في الرقابة العامة لمعالجة البيانات إلكترونياً قد تحول دون اختبار الرقابة التطبيقية المحددة لمعالجة البيانات إلكترونياً.

ثانياً: المشاكل المرتبطة بنظم معالجة البيانات المحاسبية إليكترونياً:

أدى استخدام الحاسب الآلي في تشغيل نظم البيانات المحاسبية إلى ظهور العديد من المشاكل التي لم تكن موجودة في ظل النظام اليدوي التقليدي لتشغيل البيانات المحاسبية. ويستعرض هذا الجزء بإيجاز أهم المشاكل التي أثرت على عمل المراجع الخارجي، وهي:

- التوسع في استخدام الحاسب الآلي في تطبيقات محاسبية.
- عدم وجود مستندات لبعض المدخلات.
- عدم وجود مسار مستندي واضح للمراجعة لبعض العمليات.
- عدم وجود مخرجات مرئية في بعض الأحيان.
- ضعف الحماية حول البيانات وبرامج الحاسب الآلي.
- انتشار فيروسات الحاسب.

وفيما يلي عرضاً موجزاً لهذه المشكلات:

التوسع في استخدام الحاسب الآلي في تطبيقات محاسبية:

تقوم الحاسبات الآلية بمعالجة كميات كبيرة من البيانات بسرعة وبكفاءة عالية كما أن النظم الآلية تقوم بتسجيل ومعالجة العمليات بأساليب تختلف اختلافاً واضحاً عن أساليب النظم اليدوية. وكنتيجة لذلك يحتاج المراجع الخارجي عند قيامه بمهمة المراجعة في بيئة النظم المعتمدة على الحاسب الآلي أخذ بعض الأمور في الاعتبار، منها:

-الأساليب المتوفرة له.

-توقيت عمله.

-شكل السجلات التي تحتفظ بها المنشأة.

-نظام الرقابة الداخلية.

-مدى توفر البيانات مدة بقاءها في صورة مقروءة.

عدم وجود مستندات لبعض المدخلات:

من المعروف انه في النظم الآلية يكون بالإمكان إدخال البيانات مباشرة في الحاسب الآلي دون وجود مستندات تعزز هذه المدخلات. حيث تتم عملية تسجيل وحفظ البيانات داخل وحدة الذاكرة الرئيسية للحاسب أو على أشرطة أو أسطوانات ممغنطة خارج الحاسب. فقد ترتب عليه:

-أن أصبحت البيانات المحاسبية غير مرئية وغير قابلة للقراءة والتداول مادياً كما كان الحال في النظم التقليدية.

-إمكانية تغيير البيانات المحفوظة داخل الحاسب أو على الأشرطة أو الأسطوانات الممغنطة دون ترك دليل منظور أو قرينة تدل على ذلك.

لذلك كان من الضروري إيجاد أساليب محددة للرقابة على المدخلات يكون الهدف منها توفير درجة معقولة من التأكد من سلامة المصادقة على البيانات وعدم فقدانها أو تعديلها بشكل غير مشروع.

عدم وجود مسار مستندي واضح للمراجعة لبعض العمليات:

المسار المستندي لعملية المراجعة هو "الذي يتيح إمكانية تتبع مسار العمليات المحاسبية ابتداء من المستند الأصلي وانتهاء بأثرها على القوائم المالية أو العكس".

أي البدء بالنتائج النهائية والرجوع إلى الخلف من خلال السجلات حتى الانتهاء بالمصدر. وترجع أهمية وجود مسار جيد وواضح للمراجعة بالنسبة للمراجع الخارجي في أنه يعتبر المصدر الرئيسي للحصول على أدلة وقرائن الإثبات.

غير أن استخدام نظم المعلومات المعتمدة على الحاسب الآلي قد يسبب بعض المشاكل المتعلقة بمسار المراجعة لأن معالجة البيانات تتم داخل أجهزة الحاسب الآلي مما يجعل تتبع مسار المراجعة صعباً. وقد يتم الاحتفاظ ببعض العمليات في ملفات الحاسب الآلي فقط، كما أنها قد تظل مخزونة لوقت قصير فقط. كما أن مسار المراجعة في ظل التشغيل الإلكتروني قد يكون غير مكتمل نتيجة لاختفاء بعض أجزاءه بسبب التشغيل الداخلي للحاسب. هذا بالإضافة إلى وجود بعض المشاكل التي تؤثر على مسار المراجعة والتي من أهمها ما يلي:

-عدم وجود مستندات أصلية لبعض العمليات، فقد يتم التخلص منها بعد إدخال البيانات إلى الحاسب.

-عدم وجود دفاتر يومية، حيث يتم التسجيل مباشرة في دفتر الأستاذ في بعض الأحيان.

-الملفات وقواعد البيانات داخل الحاسب الآلي غير مرئية، وبالتالي لا يمكن تتبع العمليات بوضوح من خلال مراحل النظام.

-عدم التمكن من ملاحظة التتابع والتشغيل، حيث أنه يحدث داخل أجهزة الحاسب.

والخلاصة: هي أن عدم وجود مسار مستندي جيد وواضح لعملية المراجعة سوف يؤدي إلى صعوبة تتبع العمليات، وبالتالي صعوبة اكتشاف الأخطاء أو التلاعب التي تتم من خلال الحاسب.

عدم وجود مخرجات مرئية في بعض الأحيان:

في بعض الأحيان قد لا تتم طباعة نتائج المعالجة الإلكترونية أو يتم طباعة خلاصة البيانات فقط. لذلك لا تتوافر المخرجات المرئية موضوع المراجعة، الأمر الذي يتطلب ضرورة الوصول إلى البيانات المخزونة بملفات الحاسب الآلي.

ضعف الحماية حول البيانات وبرامج الحاسب الآلي:

أدى التقدم التكنولوجي لبرامج وأجهزة الحاسبات إلى تسهيل عمليات التلاعب في البرامج وقواعد البيانات، كما أدى هذا التقدم إلى إمكانية الوصول إلى البيانات وبرامج الحاسب الآلي بسهولة، وارتكاب مخالفات أو جرائم غش، مما قد يلحق بالمنشآت المستخدمة للحاسبات خسائر كبيرة. وبصفة عامة هناك سببان ساعداً على زيادة احتمالات الغش في ظل التشغيل الإلكتروني للبيانات مقارنة بالنظام اليدوي التقليدي هما:

أ -سهولة ارتكاب الغش نتيجة للقصور في أنظمة الرقابة الداخلية أو زيادة الخبرة بتلك النظم أو الاثنين معاً.

ب -صعوبة اكتشاف وتتبع الغش نتيجة تقدم خبرة القائمين بعمليات الغش مما يمكنهم من فتح كلمات السر وإمكانية الاتصال بالنظام، مع عدم ترك قرينة منظورة أو أثر ملموس يمكن تتبعه.

انتشار فيروسات الحاسب:

أحد المشاكل الأخرى المرتبطة باستخدام الحاسبات الآلية في تشغيل نظم المعلومات المحاسبية هي فيروسات الحاسب والتي تم تعريفها على أنها:

برامج تتميز بالقدرة على تعديل البرامج الأصلية من خلال إدماج برنامج الفيروس مع البرامج الأصلية وإضفاء الصفة الرسمية على التعديلات التي يحدثها الفيروس في البرامج الأصلية، ومنع عمليات التصحيح على البرامج التي سبق تعديلها من قبل.

ثالثاً: نظم الرقابة الداخلية في ظل التشغيل الإلكتروني للبيانات المحاسبية:

الإجراءات الرقابية (مقومات نظام الرقابة الداخلية الفعال) في ظل نظم التشغيل الإلكتروني للبيانات المحاسبية.

لا تختلف مقومات نظام الرقابة الداخلية في ظل نظم تشغيل البيانات آلياً عنه في ظل النظم التقليدية اليدوية، إلا أن اختلاف طبيعة المشكلات الرقابية في كل من النظامين سوف يكون له تأثير على الإجراءات التي يجب تطبيقها لتحقيق مقومات نظام الرقابة الداخلية الفعال. وبصفة عامة تنقسم إجراءات الرقابة الداخلية في بيئة الحاسب الآلي إلى ثلاث مجموعات رئيسية هي:

1 - الإجراءات الرقابية العامة.
2 - الإجراءات الرقابية على التطبيقات.
3 - الإجراءات الرقابية على قاعدة البيانات.

وفيما يلي عرضاً موجزاً لهذه الإجراءات:

1 - الإجراءات الرقابية العامة:

هي الإجراءات التي تتصل بجميع أو معظم التطبيقات المحاسبية التي تتم بواسطة الحاسب الآلي. وتتعلق تلك الإجراءات بالرقابة على ما يلي:

أ - الفصل بين الوظائف:

يجب أن يتم فصل الوظائف في قسم المعالجة الإلكترونية للبيانات والوظائف في الأقسام المستخدمة للمعلومات. وتزداد أهمية هذا الفصل في حالة الوظائف المتعلقة بكل من:

- ✓ الصلاحيات بالتفويض.
- ✓ التنفيذ والتسجيل.
- ✓ المحافظة على الأصول.
- ✓ المسئولية المحاسبية.

فقسم المعالجة الإلكترونية يجب أن يكون مسئولاً فقط عن وظيفة التسجيل وتكون الوظائف الأخرى من مسئوليات الأقسام الأخرى داخل المنشأة.

ب -صلاحيات تفويض وتصديق عمليات تطوير، وشراء، وتغيير البرامج قبل استخدامها في معالجة البيانات:

وتشمل هذه الصلاحيات ما يلي:

✓يجب أن تتم مشاركة الأقسام المستخدمة للمعلومات في تصميم النظم جنباً إلى جنب مع قسم المعالجة الإلكترونية.

✓يجب أن يشارك موظفو الأقسام المستخدمة للمعلومات مع موظفي قسم المعالجة الإلكترونية في تجربة النظم الجديدة.

✓يجب الحصول على موافقة كل من إدارة المنشأة، الأقسام المستخدمة للمعلومات، وقسم المعالجة الإلكترونية على إدخال النظم الجديدة قبل البدء في استخدام تلك النظم.

✓ يجب إحكام الرقابة على نقل أو نسخ الملف الرئيسي أو بعض ملفات العمليات وذلك لمنع التغيير غير المسموح به في محتوياتها ولضمان دقة النتائج عند استخدام تلك الملفات.

✓يجب أن يتم التوثيق بصورة جيدة للبرامج والنظم وكذلك التغييرات التي تحدث فيها.

✓يجب توثيق مقترحات التغيير التي تتقدم بها الأقسام المستخدمة للمعلومات أو يتقدم بها قسم المعالجة الإلكترونية.

✓يجب أن يقوم مدير قسم نظم المعلومات بدراسة وتقييم جميع التغييرات التي تتم في البرامج والنظم.

✓يجب أن يتم اختبار البرامج التي يتم تعديلها باستخدام بيانات الاختبار.

✓يجب أن تتم مقارنة البرامج التي يتم تشغيلها مع النسخ المحفوظة من تلك البرامج بغرض اكتشاف أي تغييرات غير مصرح بها في تلك البرامج.

ج -صلاحيات الوصول إلى ملفات البيانات:

وتشمل هذه الصلاحيات ما يلي:

✓يجب تحديد صلاحية الوصول إلى البرامج وملفات البيانات وأجهزة الحاسب فقط في الأشخاص المفوضين بالتعامل معها كموظفي التشغيل والمشرفين عليهم وغيرهم من المسموح لهم بالوصول إلى الأجهزة والبرامج والبيانات.

✓يجب التحكم في الدخول إلى غرفة الحاسب الآلي لمنع غير المصرح لهم من دخولها.

✓يجب الاحتفاظ بسجل للزوار الذين يقومون بزيارة غرفة الحاسب الآلي بعد الإذن لهم بذلك وبمرافقته أحد الأشخاص المصرح لهم.

✓يجب استخدام الرمز الشخصي أو كلمة المرور لحصر الوصول إلى البرامج في الأشخاص المفوضين بذلك.

✓استخدام نظام الاستدعاء لتحديد وتمييز الأشخاص المفوضين بالدخول على نظام الحاسب.

✓يجب ترميز البيانات عند تخزينها في الملفات أو عند نقلها من المواقع القديمة إلى نظام الحاسب عبر الشبكات (أو غيرها).

✓منح مشغلي البرامج حرية الوصول إلى أدلة التشغيل التي تحتوي على تعليمات المعالجة مع حجب تفاصيل البرامج عنهم.

✓يجب أن يقوم فريق المراقبة بمراقبة نشاطات المشغلين وجدولة أعمالهم.

د -الإجراءات الرقابية العامة المبنية في النظام نفسه:

هناك إجراءات رقابية عامة مبنية في نظام الحاسب الآلي. وهذه الإجراءات تضفي على الحاسب ثقة قصوى من جانب من يستخدمه. وترجع هذه الثقة بشكل أساسي إلى تقدم وتطور تقنية الرقائق. والإجراءات المبنية في نظام الحاسب عبارة عن وسائل تشخيص ذاتي لاكتشاف ومنع أعطال الأجهزة.

وفيما يلي استعراض لبعض تلك الإجراءات:

▪ أجهزة وبرامج التشخيص: هي عبارة عن أجهزة وبرامج التي يوفرها صانعوا الحاسبات الآلية مع تلك الحاسبات لاستخدامها في فحص العمليات وأساليب المعالجة الإلكترونية داخل نظام الحاسب الآلي.

▪ حماية نطاق التشغيل: في معظم وحدات المعالجة المركزية يتم إجراء عدة عمليات تشغيل في وقت واحد. ولكي يتم التأكد من أن العمليات التي يتم تشغيلها في آن واحد لن تتداخل على بعضها البعض (مما يتسبب في التلف أو التغيير) فإن البرامج تحتوى على إجراءات لحماية نطاق كل عملية تشغيل.

ه -إجراءات رقابية عامة أخرى:

هناك إجراءات رقابية عامة أخرى، تتمثل فيما يلي:

✓ استخدام نظام الاحتفاظ بملفات احتياطية لاسترجاع البيانات عند التلف للمحافظة على السجلات والقدرة على تصحيح حالات الخطأ أو الفشل المفاجئ.

✓ المعالجة في الحالات الطارئة، ووضع خطط تفصيلية لمقابلة أي فشل في النظام. تفصل هذه الخطط مسئوليات الأفراد وتوضح مواقع التشغيل البديلة التي يمكن استخدامها عند الحاجة.

✓ حلقة حماية الملف، عبارة عن حلقة يتم إلصاقها بالشريط المغنط لمنع إدخال بيانات غير مصرح بها على الشريط بواسطة المشغل.

✓ بطاقات التمييز، عبارة عن ديباجة ورقية لاصقة توضع على بكرة الشريط المغنط أو أي وسيلة تخزين بيانات أخرى لتمييز الملف.

2 -الإجراءات الرقابية على التطبيقات:

يتعلق هذا النوع من الإجراءات الرقابية باستخدام الحاسب الآلي للقيام بتطبيقات محاسبية محددة. ويمكن أن تكون هذه الإجراءات إجراءات يدوية أو إجراءات إلكترونية. وتنقسم هذه الإجراءات إلى ثلاث أنواع هي:

أ -الإجراءات الرقابية على المدخلات: حيث يتم التأكد على أن البيانات التي يتم استلامها للمعالجة بالحاسب الآلي تمثل عمليات تم التصديق عليها بصورة سليمة. وأن البيانات دقيقة وصحيحة ومكتملة لحظة إدخالها في الحاسب.

ب -الإجراءات الرقابية على التشغيل (المعالجة): الغرض من هذه الإجراءات التأكيد على مصداقية ودقة المعالجة الإليكترونية للبيانات الخاصة بالتطبيق المعين. وبالتحديد تهدف تلك الإجراءات إلى التأكيد بأن جميع العمليات قد تمت معالجتها بموجب تفويض محدد، وأن جميع العمليات التي تم التصديق على معالجتها آلياً قد تمت معالجتها ولم يحذف منها شيء، وأنه لم يتم إضافة أي عمليات غير مصرح بمعالجتها إلى العمليات التي تم التصريح بمعالجتها. وتتخذ الإجراءات الرقابية على التشغيل أشكالاً عديدة منها:

✓استخدام المجاميع الرقمية: عبارة عن مجموع رقابي لا معنى له للأغراض المالية ولكنه مجموع رقمي يستخدم لأغراض الرقابة.

✓رقم الاختبار: يستخدم كوسيلة للتأكد من صحة الأرقام التي تميز حقول السجلات. فعلى سبيل المثال: استخدام رقم اختبار للتأكد من صحة أرقام حسابات العملاء في البنك.

ج -الإجراءات الرقابية على المخرجات: تهدف إلى:

✓التأكد من مصداقية وصحة المخرجات (المعلومات) التي يتم إنتاجها بعد المعالجة الإليكترونية للبيانات.

✓التأكيد بأن تلك المخرجات قد تم تسليمها إلى الموظفين المفوضين باستخدامها فقط وليس إلى أشخاص غير مصرح لهم باستخدامها.

الإجراءات الرقابية على المخرجات ذات طبيعة يدوية وليست آلية، ولذلك يطلق عليها أحياناً مسمى الإجراءات اليدوية أو إجراءات المتابعة اليدوية.

3 -الإجراءات الرقابية على قاعدة البيانات:

هناك بعض الإجراءات الرقابية الخاصة بنظم قاعدة البيانات، ومن تلك الإجراءات الرقابية:

أ -وجود إجراءات رقابية تحدد حرية الوصول إلى قاعدة البيانات فقط عن طريق الأشخاص المصرح لهم.

ب -تنسيق أنشطة مستخدمي قاعدة البيانات والتحكم فيها بحيث تكون الرقابة على البيانات متناسبة مع أهمية تلك البيانات.

ج -يقتضي اشتراك عدد كبير من المستخدمين في نفس ملفات البيانات أن تكون هناك رقابة محكمة على تلك الملفات لمنع التغيير أو الضياع.

د -اتخاذ الإجراءات الاحتياطية اللازمة للمحافظة على استمرار النظام مثل:

✓استخدام برامج الحماية اللازمة مثل الجدار الناري لمنع اقتحام الشبكة من جانب المتطفلين، وبرامج الحماية من الفيروسات.

✓وجود بيانات وبرامج احتياطية محفوظة خارج موقع العمل.

✓إجراءات محددة تتخذ في الحالات الطارئة مثل حالات السرقة والضياع للبيانات أو البرامج.

✓توفير المعالجة من خارج الشركة في حالات حدوث كوارث.

دراسة وتقويم نظام الرقابة الداخلية في ظل نظم التشغيل الإلكتروني للبيانات المحاسبية.

الهدف الأساسي الذي يسعى المراجع الخارجي إلى تحقيقه من دراسة وتقويم نظام الرقابة الداخلية هو:

-تحديد مدى الثقة في أن نظام الرقابة الداخلية المطبق في المنشأة يستطيع أن يمنع حدوث الأخطاء والغش أو يستطيع اكتشافها عند حدوثها وإجراء التصحيح اللازم.

وعلى قدر الثقة التي تتوافر لدى المراجع في أن نظام الرقابة الداخلية يستطيع منع الأخطاء والغش أو يستطيع اكتشافهما يكون حجم وتوقيت الاختبارات الأساسية التي يجريها المراجع.

لذلك فإن دراسة وتقويم نظام الرقابة الداخلية يعتبر العامل الأساسي الذي يعتمد عليه المراجع لتحديد نطاق وتوقيت الاختبارات الأساسية التي سوف يتم تطبيقها. ولا يختلف هدف المراجع من دراسة وتقويم نظام الرقابة الداخلية سواء كان يراجع حسابات منشأة تستخدم النظم الإلكترونية أو منشأة تستخدم النظم اليدوية التقليدية.

إلا أنه يجب على المراجع عند قيامه بدراسة وتقويم نظام الرقابة الداخلية في المنشآت التي تستخدم الحاسب الآلي أن يقوم بدراسة جميع الأنشطة المرتبطة بنظام الرقابة الداخلية سواء كانت تتم يدوياً أو آلياً مع ضرورة الأخذ في الاعتبار العلاقات المترابطة بين إدارة التشغيل الالكتروني والإدارات الأخرى.

ومن الجدير بالذكر أن المشكلة الأساسية التي يلاحظها المراجع في معظم المنشآت التي تستخدم الحاسب الآلي هي تركز بعض الوظائف التي قد تتصف بالتعارض في يد شخص واحد، حيث أن تركيز الوظائف في داخل إدارة التشغيل الالكتروني للبيانات يؤدي إلى الجمع بين الوظائف التي تعتبر متعارضة في ظل نظم التشغيل اليدوي التقليدي.

والحماية في هذه الحالات تتمثل في ضرورة الفصل بين صلاحيات المبرمج وصلاحيات المشغل، حيث أن الخطورة تكمن في إمكانية إجراء تعديلات على البرنامج الأصلي لتنفيذ عمليات غير مصرح بها أو تحتوي على غش أو أخطاء. فالبرنامج متى ما تم اعتماده وتطبيقه سوف يقوم بتشغيل البيانات بطريقة موحدة، إلا إذا قام أحد الأفراد القائمين على التشغيل بإدخال تعديلات على هذا البرنامج لتحقيق أهداف شخصية. ويمكن مواجهة ذلك من خلال اتخاذ إجراءات رقابية أخرى مثل وضع إجراءات رقابية إضافية، مثل رقابة الاتصال بالبرامج مثلاً تكون من خلال كلمات سرية لا يعلمها مشغلي البيانات.

وعند تقويم نظام الرقابة الداخلية في المنشآت التي تستخدم نظم معالجة البيانات إلكترونياً يقوم المراجع بتطبيق الخطوات التالية:

1 -الدراسة المبدئية للنظام:

يقوم المراجع بدراسة مبدئية للنظام بهدف تفهمه وتحديد معالمه الرقابية.

وتشمل دراسة المراجع المبدئية للنظام الخاص بالعميل:

- جميع النشاطات اليدوية والإلكترونية الهامة.
- العلاقات المترابطة بين إدارة معالجة البيانات إلكترونياً والإدارات المستخدمة أو المستفيدة لمعرفة كيفية تدفق العمليات خلال النظام.
- مدى استخدام النظام الإلكتروني في كل تطبيق من التطبيقات المحاسبية الهامة.
- الهيكل الأساسي للرقابة المحاسبية.

ويقوم المراجع بتجميع المعلومات الخاصة بدراسة النظام من خلال الاستفسارات من موظفي العميل، وملاحظة توزيع الأعمال واجراءات التشغيل، والرجوع إلى الوثائق المكتوبة كما في حالة النظام اليدوي. دراسة النظام تتم عادة باستخدام قائمة استقصاء خاصة عن نظام الرقابة الداخلية مصممة لأغراض الأنظمة الإلكترونية.

2 -تقدير نتائج الدراسة المبدئية:

يستطيع المراجع أن يقرر من خلال تقييمه للمعلومات التي حصل عليها من الدراسة المبدئية ما إذا كان سيستمر في دراسته لنظام الرقابة الداخلية أو يتوقف عن ذلك. فإذا قرر الاستمرار فإنه ينتقل إلى مرحلة استكمال الدراسة. ومن هنا يقوم المراجع باختبارات مدى تنفيذ الأنظمة الرقابية، وتقويم الإجراءات الرقابية لتحديد مدى اعتماده عليها والمدى الذي ستقتصر عليه اختباراته لتحقيق العمليات.

وقد يقرر المراجع عدم الاستمرار في دراسته لنظام الرقابة الداخلية للعميل إذا توصل إلى أحد القرارات التالية:

1)إذا قرر المراجع أن هناك ضعفاً في إجراءات الرقابة المحاسبية المتعلقة بنظام معالجة البيانات إلكترونياً بالدرجة التي تمنعه من الاعتماد على هذه الإجراءات.

في هذه الحالة:

✓لا يستمر المراجع في دراسته، ولا يقوم باختبارات مدى تنفيذ الإجراءات الرقابية وإنما يقوم بتقدير أثر نقاط الضعف التي اكتشفها على القوائم المالية واستكمال أهداف مراجعته بوسائل أخرى.

2)قد يقرر المراجع عدم استكمال دراسته المبدئية لنظام الرقابة الداخلية وعدم القيام باختبارات مدى تنفيذ الإجراءات الرقابية رغم اقتناعه بالإجراءات الرقابية.

ويحدث في الحالتين التاليتين:

✓إذا قرر المراجع أن الاختبارات الأساسية لتحقيق العمليات أقل تكلفة من استكمال دراسة الأنظمة الرقابية والقيام باختبارات مدى تنفيذ هذه الأنظمة.

✓إذا قرر المراجع أن بعض الإجراءات الرقابية المتعلقة بمعالجة البيانات إلكترونياً لا تدعو إليها الحاجة نظراً لوجود إجراءات رقابية محاسبية أخرى.

3 -إجراء اختبارات مدى تنفيذ النظام والالتزام به:

إذا قرر المراجع الاستمرار في دراسة النظام بناءاً على تقييمه لنتائج الدراسة المبدئية فإنه يقوم بإجراء اختبارات مدى تنفيذ النظام والالتزام به ليتأكد من أن الإجراءات الرقابية الموجودة يتم تطبيقها فعلاً وأنها تؤدي وظيفتها بطريقة مرضية.وتشمل هذه المرحلة:

1)اختبارات تنفيذ الإجراءات الرقابية العامة: الغرض منها تنفيذ أنظمة الرقابة الداخلية هو إعطاء تأكيد معقول بأن الإجراءات الرقابية يتم تنفيذها كما هي موضوعة.

2)اختبار إجراءات الرقابة التطبيقية: تركز على التحقق من تنفيذ برنامج الحاسب الآلي الذي سبق اعتماده دون إجراء أي تعديلات غير مصرح بها عليه ولذلك

يطلق عليها أحياناً مراجعة برامج الحاسب الآلي. وقد يتم اختبار تنفيذ إجراءات الرقابة التطبيقية بدون الحاسب أو يتم اختبارها باستخدام الحاسب.

3)الإجراءات الرقابية على قاعدة البيانات: يجب على المراجع اختبار جميع الإجراءات الرقابية لتحديد مدى اعتماده عليها والمدى الذي سيقتصر عليه اختباراته لتحقيق العمليات والأرصدة، وتشمل هذه الاختبارات الإجراءات الرقابية العامة والإجراءات الرقابية على قاعدة البيانات وإجراءات الرقابة التطبيقية.

▪ الإجراءات الرقابية العامة والإجراءات الرقابية على قاعدة البيانات فإن اختبارات المراجع لها تتم أساساً عن طريق الاستفسار والملاحظة وفحص الوثائق المختلفة.

▪ إجراءات الرقابة التطبيقية فإنها تركز على اختبار تنفيذ برامج الحاسب الآلي التي يستخدمها العميل، ذلك لأنها تشمل إجراءات الرقابة على مراحل البرنامج الثلاثة (المدخلات، عمليات التشغيل، المخرجات).

رابعاً: أساليب المراجعة في ظل التشغيل الإلكتروني للبيانات المحاسبية:

لا يختلف هدف المراجع عند مراجعة الحسابات المعدة إلكترونياً عنه في حالة مراجعة الحسابات المعدة يدوياً. ففي كل الأحوال يكون هدف المراجع هو:

-تجميع أدلة وقرائن إثبات تمكنه من إبداء رأي فني عن مدى عدالة القوائم المالية ومدى اتفاق طريقة إعدادها مع المبادئ المحاسبية المتعارف عليها.

لكن الذي يختلف هو الأساليب والإجراءات التي يتبعها المراجع لتجميع الأدلة والقرائن التي تؤيد رأيه.

إن أساليب وإجراءات المراجعة التي يتبعها المراجع عند مراجعة الحسابات المعدة بالطريقة اليدوية التقليدية، يتوافر فيها للمراجع مسار واضح للمراجعة.

أما في ظل استخدام النظم الإلكترونية لمعالجة البيانات المحاسبية فإن أشهر أساليب المراجعة هي:

1. أسلوب المراجعة حول الحاسب Auditing Around the Computer
2. أساليب المراجعة من خلال الحاسب Auditing Through the Computer

3.أساليب المراجعة باستخدام الحاسب Auditing With the Computer

وفيما يلي كيفية تطبيق هذه الأساليب:

1.أسلوب المراجعة حول الحاسب:

هذا الأسلوب لا يستخدم الحاسب الآلي كأداة للمراجعة (لذلك يطلق عليه أحياناً المراجعة بدون حاسب)

وإنما يفترض أنه إذا كانت المدخلات والمخرجات صحيحة، وتم تداول المخرجات عند خروجها من الحاسب بطريقة صحيحة، فإن العمليات والإجراءات الوسيطة في هذه الحالة يفترض أن تكون صحيحة.

ولذلك فإن إجراءات الفحص التي يقوم بها المراجع وفقاً لهذا الأسلوب تتركز على المدخلات والمخرجات فقط دون فحص عمليات التشغيل التي تتم داخل الحاسب.

وإجراءات تنفيذ هذا الأسلوب تشبه إلى حد كبير الإجراءات التي تتبع عند تطبيق إجراءات المراجعة على الحسابات المعدة وفقاً للنظم التقليدية.

لتطبيق هذا الأسلوب يختار المراجع عينة من العمليات ويتتبعها ابتداءً من المستندات الأولية حتى انتهاءها في القوائم المالية ويقارن النتائج التي يتوصل إليها مع النتائج (المخرجات) المطبوعة المستخرجة من الحاسب.

مهمة المراجع هي مقارنة مخرجات الحاسب مع المستندات الأصلية والمجاميع الرقابية بهدف اختبار مدى دقة التشغيل، وذلك دون الاعتماد على الضوابط الإلكترونية، حيث ينظر المراجع عند تطبيقه لهذا الأسلوب إلى الحاسب على أنه صندوق مغلق لا يهتم بما يحدث داخله وإنما يركز على فحص العلاقة بين المدخلات والمخروجات.

يفرض هذا الأسلوب على المراجع ضرورة الإطلاع على:

✓مستندات كافية أصليه. (ضرورة أن تكون المستندات بيد المراجع قبل إدخالها في لغة الحاسب).

✓قائمة شاملة بمخرجات النظام في صورة قوائم يسهل قراءتها. (صياغة المخرجات بصورة تفصيلية كافية بحيث يتمكن المراجع من تتبع العمليات).

يناسب هذا الأسلوب الحالات التي تكون:

✓الأنظمة فيها في مراحلها الأولى والتي يمكن في ظلها أن يتم التشغيل الإلكتروني إلى جانب التشغيل اليدوي.

✓الأنظمة الصغيرة المبسطة.

إلا أنه قد لا يصلح في حالات نظم التشغيل الإلكتروني المتطورة والمعقدة حيث يكون هناك أكثر من نظام وهناك علاقات متداخلة بين كل الأنظمة حيث تعتبر مخرجات أحد النظم مدخلات لنظام أخر.

2.أساليب المراجعة من خلال الحاسب:

يتلخص هذا الأسلوب في قيام المراجع بفحص واختبار عملية تشغيل البيانات داخل الحاسب بالإضافة إلى التأكد من صحة المدخلات والمخرجات، فأسلوب المراجعة من خلال الحاسب على عكس أسلوب المراجعة حول الحاسب، لا يتجاهل وجود الحاسب بل يأخذه في الاعتبار ويستخدمه في عملية المراجعة

ويركز على مدى الالتزام بالبرنامج المعين وهو الأمر الذي يتطلب من المراجع قدراً مناسباً من المعرفة بالحاسب ونظم التشغيل الإلكتروني للبيانات وتصميم البرامج واستخدامها.

هناك عدة أساليب تشترك في استخدام الحاسب لتنفيذ عمليات الفحص والتحقق من صحة العمليات والأرصدة. تتفق هذه الأساليب في الافتراض الذي تنبني عليه وهو أنه

إذا كانت عمليات تشغيل البيانات تتم بشكل دقيق فإن ذلك يعني أن هنالك احتمال كبير لأن تكون السجلات المحاسبية وبالتالي القوائم المالية صحيحة.

يصلح هذا الأسلوب لمراجعة النظم المتطورة والتي تقل فيها درجة الاعتماد على النسخ المطبوعة للمخرجات، وهو الأمر الذي يفرض على المراجع ضرورة تنفيذ مهمته في التحقق من صحة العمليات والأرصدة من خلال الحاسب وليس حول الحاسب.

يستخدم هذا الأسلوب في مجالين:

✓ مجال التحقق من أوجه التشغيل، (أي التأكد من الالتزام بوسائل الرقابة ومن صحة البرامج) بمعنى التحقق من أن البرامج التي تستخدم بالفعل في عملية المعالجة هي نفس البرامج المصرح بها (الالتزام بالبرامج) وأنه لم تحدث عليها تعديلات غير مصرح بها.

✓ مجال التحقق من صحة ودقة النتائج المتولدة من تشغيل البيانات، وذلك عن طريق استخدام الحاسب في إجراء الاختبارات الأساسية.

3.أساليب المراجعة باستخدام الحاسب:

يقصد بالمراجعة باستخدام الحاسب (يسمى أيضاً المراجعة بمساعدة الحاسب) أن الحاسب وبرامجه تستخدم كأداة من أدوات المراجعة.

نص معيار المراجعة في المنشآت التي تستخدم الحاسب الآلي على أنه يجب على المراجع أن يأخذ في الاعتبار "استخدام طرق المراجعة بمساعدة الحاسب الآلي لزيادة فاعلية تنفيذ إجراءات المراجعة، حيث يوفر استخدام طرق المراجعة بمساعدة الحاسب الآلي لمراجع الحسابات الفرصة لتطبيق إجراءات معينة على كل الحسابات أو كل العمليات. بالإضافة إلى ذلك ففي بعض الأنظمة المحاسبية قد يواجه مراجع الحسابات صعوبة أو استحالة تحليل بيانات معينة أو اختبار إجراءات رقابية معينة بدون مساعدة الحاسب الآلي".

في ظل هذا الأسلوب ينظر المراجع إلى الحاسب وبرامجه كمساعدين له عند أداء اختبارات مدى الالتزام والاختبارات الأساسية، ولذا يسمى هذا الأسلوب أيضاً المراجعة بمساعدة الحاسب.

يعتمد هذا الأسلوب على استخدام حزم برامج المراجعة التي تضم برنامج أو أكثر مصمم لإنجاز واختبار وظائف تشغيل البيانات.

أمثلة على استخدام هذا الأسلوب:

✓ مجال تطبيقات المعاينة الإحصائية في إنجاز اختبارات المراجعة.

مجال فحص حسابات العملاء. (استخدام الحاسب في اختبارات مدى الالتزام لأرصدة العملاء، وإعداد مصادقات العملاء)

الفصل السادس

مدى ملاءمة مهنة المحاسبة لبيئة التجارة الإلكترونية

الفصل السادس

مدى ملاءمة مهنة المحاسبة لبيئة التجارة الإلكترونية

هدفت هذه الدراسة إلى، التعرف على بيئة التجارة الإلكترونية، ومقارنة بيئة التجارة التقليدية ببيئة التجارة الإلكترونية، ومن ثم تحديد فيما إذا كانت السياسات المحاسبية المعمول بها تلائم البيئة التجارية الجديدة المتمثلة بالتجارة الإلكترونية، وتحديد المشاكل التي تحدد مهنة المحاسبة مع التعامل مع البيئة التجارية الجديدة، ومحاولة حل تلك المشاكل إن وجدت.

لقد توصل الباحثان إلى ما يلي:

1 -التجارة الإلكترونية تؤثر على مهنتي المحاسبة والتدقيق.

2 -تعمل التجارة الإلكترونية في بيئة غير ملموسة وفريدة من نوعها، وتفتقد إلى التوثيق المستندي.

3 -نظرا لتلك البيئة الفريدة التي تفتقد إلى التوثيق المستندي، فان مهنتي المحاسبة والتدقيق توجهان المشاكل التالية:

- عدم وجود آلية محددة للاعتراف بالإيرادات المتولدة عبر التجارة الإلكترونية.
- عدم وجود آلية محددة للتخصيصي الضريبي.

4 -فشلت النظرية المحاسبية الحالية بالتعامل مع مشكلة الاعتراف بإيرادات التجارة الإلكترونية.

5 -يمكن حل المشاكل المرافقة للتجارة الإلكترونية من خلال تطوير سياسات وإجراءات محاسبية تكنولوجية تستطيع توفير الأمان، والتوكيدية، والموثوقية لمخرجات نظام المعلومات المحاسبي.

أخيرا، فقد تمكن الباحثان من اقتراح نقطة جديدة للاعتراف بإيرادات التجارة الإلكترونية، واسماها "نقطة الاعتراف عند تحقق الأمان لعمليات النظام" والتي يمكن تلبيتها إذا تمكنا من تحقيق التالي:

- أمان العمليات "وذلك من خلال تطوير نظام، يربط نظام المعلومات المحاسبي الخاص بالشركة مع موقعها الإلكتروني على شبكة الانترنيت، بحيث يتضمن نظام الربط كل من السياسات والإجراءات المحاسبية الكفيلة بتوفير كل من الأمان، والموثوقية، والتوكيدية لمخرجات نظام المعلومات المحاسبي.

- إجراءات تأكيد الأمان "وذلك من حلال تعين جهة خارجية مؤهلة لتدقيق السياسات والإجراءات التي يفترض بها توفير الأمان، والتوكيدية، والموثوقية لمخرجات نظام المعلومات المحاسبي.

لقد تمكن اختراع شبكة الاتصالات المعقدة الحديثة والمتمثل بشبكة الانترنت من إزالة الحدود بين جميع دول العالم ، وجعل العالم أشبه بالقرية الواحدة ، وظهر ضمن هذا الاختراع آليات وأدوات تعامل متعددة الأشكال والأغراض.

وتعد أداة أو آلية التجارة الإلكترونية إحدى الأدوات الحديثة التي أفرزتها شبكة الانترنيت ، ورافق ظهورها تغير جوهري ببيئة الأعمال الخاصة بها ، فمن جهة هي أداة ذات طابع غير ملموس ، ومن جهة أخرى ونظرا لطابعها الفريد من نوعه رافقها غياب التوثيق المستندي لأغلب مراحل العمليات التجارية التي تتم من خلالها.

سيحاول الباحثان في هذه الدراسة شرح طبيعة وماهية التجارة الإلكترونية وتوضيح الفرق بينها وبين التجارة التقليدية ، ومن ثم إظهار أثرها على بيئة الأعمال الخاصة بها ، وكيف أن البيئة الجديدة للأعمال أحدثت وستحدث تغييرات كبيرة على مهنتي المحاسبة والتدقيق.

وانطلاقا من مفهوم أن كلا من مهنة المحاسبة والتدقيق تؤثر وتتأثر بالبيئة التي تعمل بها ، سيقوم الباحثان بمحاولة شرح العلاقة المتولدة بين بيئة التجارة الإلكترونية ، ومهنة المحاسبة والتدقيق من جهة ، وبينها وبين معايير المحاسبة والتدقيق من جهة أخرى.

كما سيتطرق الباحثان إلى المخاطر المرافقة للتجارة الإلكترونية ، ومسبباتها وكيفية تفاديها ، ومدى تأثير هذه المخاطر على آلية الاعتراف بالإيراد محاولين

إيجاد حلول مناسبة تساعد باستغلال التجارة الإلكترونية بشكل آمن والاستفادة منها بشكل يخدم المتعاملين بها.

لقد عملت مهنة المحاسبة ومنذ نشأتها في بيئة تجارية ذات طابع يتسم بالبطء وقليل التغير إلى أن ظهرت بيئة التجارة الإلكترونية، والتي تتسم بعدت سمات جديدة مثل التسارع الكبير في تطورها، وهيكلها غير الملموس، وغياب الأمان لأغلب العمليات التجارية التي تتم من خلالها، وكذلك غياب التوثيق المستندي لأغلب عملياتها.

من الملاحظ بأن جميع السياسات المحاسبية أنشأت وطورت للتعامل مع البيئة التجارية التقليدية، وسعى دوما المشرع لتلك السياسات إلى تمكين النظام المحاسبي من الخروج بمعلومات تتمتع بما اتفق على تسميته الخصائص النوعية للمعلومات المحاسبية، وتوفير خاصتي الملاءمة والثقة لتلك المعلومات كي تحوز على رضا أصحاب المصالح وبالتالي اعتمادها أساسا موثوقا به لبناء واتخاذ قراراتهم المستقبلية المتعددة الأغراض.

والسؤال الذي يطرح نفسه، وبقوة، هل تلك السياسات المحاسبية التي أنشأت في ظل بيئة تجارية تقليدية، تصلح، ويمكن استخدامها في ظل البيئة التجارية الإلكترونية الحديثة؟

وسيسعى الباحثان كذلك إلى التعرف على البيئة التجارية الجديدة المتمثلة بالتجارة الإلكترونية، ومقارنتها بالبيئة التجارية التقليدية، ومن ثم معرفة مدى كفاية وملاءمة السياسات المحاسبية للتعامل مع البيئة الجديدة، وحصر المشاكل التي تواجهها مهنة المحاسبة في ظل البيئة التجارية الجديدة إن وجدت، واقتراح بعض التوصيات الكفيلة بحل تلك المشاكل.

أهداف الدراسة

تهدف هذه الدراسة إلى ما يلي:

1- التعرف على البيئة التجارية الجديدة المتمثلة بالتجارة الإلكترونية.

2- مقارنة البيئة التجارية التقليدية بالبيئة التجارية الجديدة المتمثلة بالتجارة الإلكترونية.

3- معرفة مدى كفاية وملاءمة السياسات المحاسبية للتعامل مع البيئة الجديدة المتمثلة بالتجارة الإلكترونية.

4- حصر المشاكل التي تواجهها مهنة المحاسبة في ظل البيئة التجارية الجديدة المتمثلة بالتجارة الإلكترونية إن وجدت.

5- اقتراح بعض التوصيات الكفيلة بحل تلك المشاكل.

أهمية الدراسة

تنبع أهمية الدراسة من أهمية مهنة المحاسبة نفسها، وأهمية التجارة الإلكترونية والدور الذي تلعبانه في بيئة الأعمال التي تعد ركيزة أي اقتصاد في أي دولة وبما أن مهنة المحاسبة تعتبر العامود الفقري لأي منشأة ويتم اعتماد نتائجها كأساس في اتخاذ القرارات، فبالتالي فإن معرفة دورها الجديدة ومدى نجاعته في التعامل مع البيئة التجارية الجديدة، ومحاولة حل المشاكل المرافقة لهذا الدور الجديد إن وجدت سيساهم بشكل جوهري في تقوية الاقتصاد، وذلك من خلال إضفاء خاصتي الملاءمة والثقة للمعلومات المحاسبية المتعلقة بتعاملات البيئة التجارية الجديدة المتمثلة بالتجارة الإلكترونية .

مشكلة الدراسة

كما هو معروف بأن إيرادات التجارة الإلكترونية إيرادات ضخمة جدا بشكل كان يصعب على العقل تصورها، والسبب الرئيسي في ضخامة تلك الايرادات بأن عمليات التجارة الإلكترونية تتم عبر شبكة الانترنيت التي استطاعت إلغاء الحدود الاقتصادية بين الدول. لقد استطاعت الدول المتقدمة استغلال تقنية التجارة الإلكترونية بشكل مثالي واخترقت أسواق العالم بشكل منقطع النظير، وبدأت تحقق إيرادات ضخمة جدا، ورغم السلبيات الكثيرة المرافقة للتجارة الإلكترونية والمؤثرة بشكل كبير على النظام المحاسبي، إلا أن شركات الدول المتقدمة تحاول وبشكل دؤوب

تقليص تلك السلبيات بشتى الوسائل نظرا لما تحققه التجارة الإلكترونية من عوائد ضخمة لها بشكل خاص ولدولها بشكل عام.

وبالتالي فان استطاع الباحثان الإجابة على عدة تساؤلات جوهرية، قد يساهما ولو بشكل متواضع من حث الشركات الأردنية على الخوض بهذا النوع من التجارة المجزي، وتبديد مخاوفها من السلبيات المرافقة لها بشكل عام، ومن السلبيات المؤثرة على النظام المحاسبي الخاص بها بشكل خاص.

وبناءا على ما تقدم يمكن حصر مشكلة الدراسة بالسؤال الجوهري التالي:

1- هل هناك مشاكل تواجه مهنة المحاسبة في ظل البيئة التجارية الجديدة المتمثلة بالتجارة الإلكترونية؟ وما هي الحلول اللازمة لحل تلك المشاكل؟

محددات الدراسة

يعتقد الباحثان بأن من أهم محددات الدراسة ما يلي:

1- حداثة الموضوع.
2- عدم إفصاح الشركات المستخدمة للتجارة الإلكترونية عن المشاكل التي تواجه نظامها المحاسبي خوفا من فقدان الثقة بها من قبل المتعاملين معها.
3- قلة البحوث المتعلقة بالموضوع.
4- عدم وجود شركات في الأردن تتعامل بالتجارة الإلكترونية على نطاق واسع.

مصادر الدراسة

تتكون مصادر الدراسة من مصادر ثانوية كالتالي:

المصادر الثانوية:

سيتم التركيز على جميع المصادر الممكنة من خلال المواقع المتوفرة على شبكة الانترنيت، وذلك بالتركيز على بعض مواقع مشرعي السياسات المحاسبية بشكل عام، وعلى مواقع الدوريات العالمية ومواقع الجامعات بشكل خاص، وذلك لاستقاء أحدث المعلومات والمستجدات بموضوع الدراسة.

التجارة الإلكترونية

- شبكة الانترنيت العالمية Internet :

هي عبارة عن شبكة اتصالات عالمية تربط بين ملايين شبكات الاتصال وملايين أجهزة الكمبيوتر بشتى أشكالها وأنواعها .[1]

- الشبكة العنكبوتية العالمية WWW :

وهي إحدى الخدمات المشهورة التي توفرها شبكة الانترنيت العالمية والتي تساعد على الدخول إلى مليارات المواقع الموجودة على الشبكة[2].

التجارة الإلكترونية E-commerce

يمكن القول بأن مصطلح التجارة الإلكترونية ببساطة يعني استخدام الانترنيت والشبكة العنكبوتية العالمية لتبادل العمليات بشتى أشكالها بين الأعمال المختلفة مع التركيز على استخدام التكنولوجيا الرقمية في العمليات التجارية بين الشركات والأفراد[3] .

وقد عرفها البعض بأنها " المعاملات التجارية التي تتم من قبل الأفراد والهيئات والتي تعتمد على معالجة ونقل البيانات الرقمية ، بما فيها الصوت والصورة من خلال شبكات مفتوحة مثل الانترنيت أو مغلقة ، والتي تسمح بالدخول إلى الشبكات المفتوحة "[4].

وفي التجارة الإلكترونية لا بد من التطرق لعدة تعاريف أخرى ، ومن أهمها التالي:

- العمليات الرقمية Digitally Enabled Transactions وهي جميع العمليات التي تتم بوسائط تكنولوجيا رقمية ، والتي في اغلبها تتم عبر شبكة الانترنيت والشبكة العنكبوتية العالمية .

[1] Kenneth C. Laudon & Carol Guericio Traver, E-commerce, by Eyewire, USA, 2001, P. (109) .

[2] Ibid., P. (109) .

[3] Ibid., P. (7) .

[4] زايري بلقاسم ودلوباشي علي ، طبيعة التجارة الإلكترونية وتطبيقاتها المتعددة ، المؤتمر العلمي السنوي الثاني لتكنولوجيا المعلومات ودورها في التنمية الاقتصادية ، كلية الاقتصاد والعلوم الإدارية ، جامعة الزيتونة 6-8 أيار _مايو) 2002 ، صفحة رقم 360 .

- العمليات التجارية Commercial Transactions وتعني هنا العمليات التجارية التي تتضمن تبادل القيم (والمتمثلة بوسائط النقد المختلفة: كالأموال وبطاقات الاعتماد والشيكات) بين الشركات والأفراد مقابل بضائع أو خدمات.

الفرق بين التجارة الإلكترونية E-commerce والأعمال الإلكترونية E-business

لقد ظهر خلاف وجدل حول تعريف التجارة الإلكترونية والأعمال الإلكترونية وأيهما يندرج تحت الآخر ، فالرأي الأول يعتقد بأن التجارة الإلكترونية تشمل جميع العمليات الإلكترونية التي تقوم بها الشركات متضمنة كذلك البنية التحتية لنظم معلومات المنشأة وتضم بالتالي الأعمال الإلكترونية ، وحسب هذا الرأي[1] فإن الأعمال الإلكترونية عبارة عن العمليات الرقمية الإلكترونية ضمن بيئة المنشأة فقط ، ويقتصر دورها ضمن إجراءات الرقابة الداخلية وكمثال عليها ، عملية السيطرة والاطلاع على حيثيات مخزون الشركة الموجود في موقع بعيد من خلال وسائط تكنولوجيا رقمية . أما الرأي الثاني، فيعتقد بأن الأعمال الإلكترونية هي الأشمل ويندرج تحتها جميع أدوات التعامل الإلكترونية الأخرى .

ويرى الباحثان بأنه من الأنسب اعتماد الرأي الأول لأغراض إكمال الدراسة من منطلق أن الرأي الأول أقرب للصحة ، فمن جهة ، تطلق جميع الشركات العالمية المتعاملة عبر شبكة الانترنيت على جميع تعاملاتها الإلكترونية عبر شبكة الانترنيت مسمى التجارة الإلكترونية ، ومن جهة أخرى، يتفق الرأي الأول وبدرجة كبيرة مع العقلية الإدارية والمحاسبية فمصطلح الأعمال Business يندرج على المنشأة كوحدة مستقلة ، والهدف من إنشائها هو إدارة عمل محدد لتحقيق ربح ، والتجارة Commerce تدل على التعاملات مع الغير لإنجاح العمل الذي تم إنشاؤه.

---

[1]Kenneth C. Laudon, Oipcit., P. (109) .

أهمية التجارة الإلكترونية

يمكن القول إن التجارة الإلكترونية تعد من أهم اختراعات العصر والتي يمكن من خلالها تحقيق أرباح لم يكن من الممكن تحقيقها سابقا بالطرق التقليدية والسبب يعود للأمور التالية :

1 -انخفاض التكلفة ، كانت عملية التسويق للمنتج مكلفة جدا في السابق حيث إن الإعلان عن المنتج كان يتم بواسطة الوسائل التقليدية عبر التلفاز والجرائد ، أما الآن فيمكن تسويقه عبر شبكة الانترنيت وبتكلفة ضئيلة جدا .

2 -تجاوز حدود الدولة ، كانت الشركة تتعامل مع عملاء محليين فقط بالسابق وإن رغبت في الوصول إلى عملاء دوليين كانت تتكبد مصاريف كبيرة وغير مضمونة العائد ، أما الآن فتستطيع الشركة أن تضمن اطلاع الجميع على منتجاتها دون أي تكلفة إضافية تذكر ، خاصة أن شبكة الانترنيت دخلت جميع الدول.

3 -التحرر من القيود ، سابقا كانت الشركة تحتاج إلى ترخيص معين والخضوع لقوانين عديدة وتكبد تكلفة إنشاء فرع جديد أو توكيل الغير في الدولة الأجنبية حتى تتمكن من بيع منتجاتها ، أما الآن لم يعد أي من تلك الإجراءات ضروريا .

ولمعرفة المزيد عن أهمية التجارة الإلكترونية ، يمكن الاطلاع على المميزات الفريدة التي تتمتع بها .

المميزات الفريدة لتقنية التجارة الإلكترونية [1]

تتمتع تقنية التجارة الإلكترونية عن غيرها من التقنيات التقليدية بعدة مميزات ومن أهمها التالي :

1 -الوجود الواسع Ubiquity ، من منطلق أن التجارة الإلكترونية متواجدة في كل مكان وفي كل الأوقات ، فالتجارة التقليدية بحاجة إلى سوق ملموس يستطيع المتعامل الذهاب إليه للشراء ، أما التجارة الإلكترونية فإنها لا تحتاج إلى سوق ملموس ويستطيع المتعامل من خلالها الدخول إلى هذا السوق غير الملموس في أي وقت ومن أي مكان بوساطة الكمبيوتر وبلمسة بسيطة على الموقع الذي يرغب بزيارته ، وبضغط عدة أزرار يمكنه الإطلاع على المنتج وشرائه .

2 -التداول العالمي Global Reach ، تمكن التجارة الإلكترونية المتعاملين من خلالها تخطي حدود الدول والوصول إلى أي مكان بالعالم وبضغطة زر بسيطة على الكمبيوتر ودون تكلفة تذكر ، على النقيض من التجارة التقليدية التي يقتصر التعامل بها محليا ويصعب على المتعاملين زيارة الأسواق العالمية للتسوق.

3 -معايير عالمية Universal Standards ، وهي مقاييس أو معايير شبكة الانترنيت ، التي يتم من خلالها تعاملات التجارة الإلكترونية وبشكل موحد بين دول العالم ، أما التجارة التقليدية فتخضع لمعايير ومقاييس محلية تعتمد على الدولة نفسها ، فمقاييس التجارة الإلكترونية تخفض تكلفة الدخول إلى أسواق المنتجات بشتى أشكالها ، بينما مقاييس التجارة التقليدية خاضعة لسياسات الدول وتكلفة دخول أسواق تلك الدول تختلف من دولة إلى أخرى .

4 -موارد معلومات غنية Information Richness ، فالتجارة الإلكترونية ومن منطلق تمكنها من الوصول لجميع المستهلكين وفي شتى أنحاء العالم تزود المستهلك بمعلومات كثيرة ، بواسطة استخدام الشركات لجميع وسائط التكنولوجيا الرقمية ، كالوسائط المسموعة والمقروءة والمرئية ، بينما في التجارة

[1]Kenneth C. Laudon & Carol Guericio Traver, Opicit., P. (9) .

التقليدية كانت آلية تزويد المعلومة تعتمد وبشكل رئيسي على مقابلة المستهلك وجها لوجه .

5 -التواصل Interactivity ، تعد التجارة الإلكترونية آلية تواصل ذات فاعلية عالية جدا ، من منطلق أنها وسيلة اتصال ذات اتجاهين بين العميل والتاجر وعلى سبيل المثال لا الحصر ، تفتقد التجارة التقليدية لهذا النوع من الاتصالات فلو أن إحدى الشركات أعلنت عن بضائعها عبر التلفاز ، فمن غير الممكن أن يتواصل العميل مع المعلن عبر الجهاز ، ولكن هذا التواصل اصبح ممكنا عبر التجارة الإلكترونية .

6 -كثافة المعلومات Information Density ، من المعروف بأن شبكة الانترنيت جعلت المعلومات كثيفة وذات نوعية ممتازة وحديثة ، وبشكل مشابه قللت التجارة الإلكترونية من آلية البحث عن المعلومات والتخزين ومن تكلفة الاتصالات من جهة ، ومن جهة أخرى زادت هذه التقنية من التوقيت الملائم للمعلومة Timeliness ودقتها كذلك.

7 -الاستهداف الشخصي Personalization ، من منطلق أن التجارة الإلكترونية تمكن المسوق للمنتج من استهداف فئة معينة من الأفراد من خلال تعديل الإعلانات عبر الشبكة ، وذلك بتحديد معلومات الفرد المرغوب اطلاعه على المنتج كتحديد العمر ، والجنس ، وطبيعة عمله وأي أمور أخرى يراها المسوق ضرورية.

أنواع التجارة الإلكترونية[11]

هناك عدة أنواع من التجارة الإلكترونية ، والتي لا بد من التعرف عليها ومن أهمها:

1 -التعامل بين التاجر والمستهلك Business-to-Consumer (B2C)

ويعد هذا النوع من التجارة الإلكترونية من أهم الأنواع والذي يحاول التاجر من خلاله الوصول للأفراد المستهلكين ، ويحتوي هذا النوع على عدة نماذج والتي

[11]Kenneth C. Laudon, Ibid., Page (13) .

سيتم التطرق إليها لاحقا؛ وذلك لأهميتها القصوى وترابطها الوثيق مع جوهر هذه الدراسة.

2 -التعامل بين تاجر وتاجر آخر Business-to-Business (B2B) ، حيث يركز هذا النوع من التجارة الإلكترونية على بيع المنتجات من تاجر إلى تاجر آخر.

3 -التعامل بين مستهلك ومستهلك آخر Consumer-to-Consumer (C2C) ، حيث يساعد هذا النوع من التجارة الإلكترونية الأفراد بأن يبيعوا لبعضهم البعض ، وذلك من خلال المزادات التي تبنى في شبكة الانترنيت.

4 -التعامل بين مستخدم ومستخدم آخر Peer-to-Peer (P2P) ، يعمل هذا النوع على تمكين مستخدمي الانترنيت على تبادل المعلومات ، والاتصال فيما بينهم دون وجود وسطاء ، ومن ثم الاتفاق على أية صفقات تجارية تتم حسب الشروط المتفق عليها ، وقد أوجدت برامج خاصة لهذه الغاية والتي تمكن مستخدميها ، تجاريون كانوا أم غيرهم بتبادل أطراف الحديث (Chatting) بصور كتابية وسمعية ومرئية.

5 -التجارة الإلكترونية عبر جهاز الهاتف النقال Mobile Commerce ، يعد هذا النوع من التجارة الإلكترونية من أحدث الأنواع ، حيث يتم بواسطته استخدام أجهزة هاتف نقال رقمية مصممة بشكل يمكنها من الاتصال بشبكة الانترنيت من خلال مزود الخدمة والوصول لأي موقع معين والاطلاع على السلع المعروضة وإجراء عملية الشراء.

بناء نموذج تجارة إلكترونية على شبكة الانترنيت [1]

من المعروف بأن أية شركة ترغب في دخول هذا النوع من آليات التسويق والبيع لا بد لها من تقييم الأمور بشكل مناسب ومن ثم اتخاذ القرار المناسب. ولعمل ذلك لا بد لها من إنشاء ما يسمى نموذج أعمال Business Model وهو عبارة عن تحديد مجموعة من الفعاليات المخطط لها لإنتاج أرباح مستهدفة في السوق .

ولكي تتمكن أي شركة من إنشاء ذلك النموذج لا بد من أخذ العناصر والنماذج التالية بالحسبان:

1 -عرض قيمة Value Proposition ، وهو معرفة الشركة بآلية تلبية رغبات زبائنها ، وذلك من خلال الإجابة على عدة تساؤلات ، لماذا يفضل المستهلك التعامل مع شركتك دون الشركات الأخرى؟ وما هي الأمور التي يمكن أن تزودها شركتك للمستهلك ويعجز الآخرون عن تزويده بها ؟

2 -نموذج الإيراد Revenue Model ، ويمكن تسميته كذلك النموذج المالي Financial Model وهو الذي يشرح كيفية تحقيق الشركة للعوائد ، وكيفية تحقيق الربحية ، وما هي الآليات التي ستضمن استغلال رأس المال المستثمر بأفضل الطرق لتحقيق أفضل العوائد؟ ويمكن أن يتضمن هذا النموذج عدة نماذج أخرى والتي من أهمها التالي:

- نموذج إعلان إيرادي Advertising Revenue Model ، يوضح أو يبين هذا النموذج ، كيفية إنشاء موقع خاص بالشركة على شبكة الانترنيت للإعلان عن منتجها مقابل رسوم معينة، وكيفية إدراج منتجها والإعلان عنه عبر المواقع الأخرى المتعددة.

- نموذج اشتراك إيرادي Subscription Revenue Model ، وهي الآلية التي يجب أن تتبعها الشركة بتوفير خدمات أخرى في موقعها، والتي قد يرغب بها الجمهور مقابل مبالغ بسيطة وقد تكون مجانية أحيانا، مثل فتح بريد إلكتروني مجاني للمتعاملين معها أو توفير برامج مجانية لهم أو اشتراكات في مواقع ترفيهية

---

[1] Kenneth C. Laudon & Carol Guericio, Ibid., P. (57) .

مقابل رسوم ضئيلة ، والغاية من هذه الخدمة ، هو تشجيع المتعاملين معها على شراء منتجها والذي سيضمن لهم الحصول على خدمات أخرى مجانية أو برسوم ضئيلة وكلما كانت هذه الخدمات أكثر ، رغب المستهلك بشراء منتجها .

- نموذج البيع الإيرادي Sales Revenue Model ، وهو النموذج الرئيسي على موقع الشركة والذي يتضمن جميع التفصيلات الضرورية عن منتجات الشركة وأنواعها وأصنافها ، ويتضمن كذلك آلية طلب المنتج وآلية الدفع والشروط الأخرى المحددة مسبقا من قبل الشركة. وكمثال حي على ذلك موقع شركة Amazon.com التي تقوم على بيع الكتب بشكل رئيسي ، فلو دخلنا إلى ذلك الموقع لوجدنا تفاصيل كافية عن جميع الكتب المتوفرة لديها وبتفصيلات عديدة .

3 -سماسرة العمليات Transaction Brokers ، يوجد مواقع على الشبكة لمن يسمون بسماسرة العمليات واللذين ينصب عملهم على الإعلان عن منتجات الغير مقابل عمولة محددة على العمليات التي تتم من خلالهم ومن الضروري جدا للشركة الإعلان عن منتجها عبر مواقعهم ، والسبب يكمن في أن موقع الشركة في الغالب يكون مجهولا لمستخدمي شبكة الانترنيت ، وحيث أن مواقع السماسرة تكون في الغالب مواقع مشهورة جدا فيفضل الإعلان كذلك من خلال هذه المواقع.

4 -منشئو الأسواق Market Creators ، وهم الذين ينشؤون بيئة رقمية محددة عبر شبكات الانترنيت تمكن التقاء كل من البائع والمشتري ، وهذه البيئة عبارة عن برامج بحث رقمية ، فعلى سبيل المثال، لو رغب أحد مستخدمي الانترنيت البحث عن كتاب محدد في المحاسبة ، فيمكنه دخول أحد مواقع منشئي الأسواق المعروفة مثل: Yahoo.com ، وسيجد في داخل الموقع منطقة بحث فارغة كتب بجانبها Search ، يقوم بكتابة الاسم المراد البحث عنه ، وفي حالتنا هذه سيقوم بكتابة Accounting Book ، ويضغط على آلية البحث وسيقوم الموقع خلال فترة قصيرة جدا بفتح عناوين الشركات التي تملك كتب المحاسبة وما على المستخدم سوى الضغط على اسم الموقع ليفتح أمامه ويرى ما بداخله .

5 -مزودو الخدمة Service Provider ، هنالك مواقع مشهورة جدا تسمى مزودو الخدمة، وهي باختصار مواقع مشهورة ومعروفة لأغلب متعاملي الانترنيت متخصصة بنوع معين من الخدمات ، أو بمعنى آخر مرتبطة بمزودي هذه الخدمات فعلى سبيل، المثال لو كانت الشركة متخصصة بتصليح السيارات فمن مصلحتها الاشتراك بمواقع خدمة تصليح السيارات ، حيث سيدرج اسم الشركة في ذلك الموقع وذلك لأن المهتم بتصليح سيارته سيقصد الموقع العام لخدمة تصليح السيارات للاطلاع على الشركات المتخصصة بذلك المجال .

علاقة التجارة الإلكترونية بعلم المحاسبة

إن جميع الهيئات والجمعيات المحاسبية وتدقيق الحسابات المهتمة بعلم المحاسبة تولي التجارة الإلكترونية اهتماما كبيرا جدا ، من منطلق أن عملية البيع التي تتم من خلال موقع الشركة مرتبطة بشكل وثيق ومباشر بنظام المحاسبة المؤتمت ، وقد اصبح حتميا على المحاسب والمدقق الإلمام بهذا العلم الجديد . فلقد ذكر (البرت مرسيلا Albert Marcella) في مقالته المعنونة بالتجارة الإلكترونية في مجلة تدقيق تكنولوجيا المعلومات ، " لقد أحدثت التجارة الإلكترونية تغيرات كبيرة في علم التجارة العالمي وفي آلية العمليات التجارية مما جعل من الضروري أن يلم كل من المحاسب والمدقق بتلك التغيرات وأثرها على مهنتيها وعلى الأعمال التي يقومون عليها وعلى ظروف البيئة القانونية المتعلقة بالمهنة " [1]

من المهم هنا أن نذكر بأن التجارة الإلكترونية وشبكة الانترنيت تستطيع أن تساهم بالخصائص النوعية للمعلومات ، وذلك بتوفير خاصية الملاءمة بشكل كبير وخصوصا بتوفير الخاصية الفرعية المتمثلة بالتوقيت المناسب. ويعتقد الباحثان أن النظام المحاسبي ، وبما يزوده من معلومات هامة جدا لأصحاب المصالح بشكل عام ومتخذي القرار بشكل خاص ، يصبح عديم الجدوى في حالة عدم توفر الثقة في تلك

[1] Albert Marcella, Electronic Commerce, Part 1, IT Audit, Vol. 1, September 1, 1998, Institute of internal auditors - https://theiia.org .

المعلومات ، وبما أن نظام التجارة الإلكتروني والمرتبط بشبكة الانترنيت مربوط بشكل مباشر بنظام المحاسبة المؤتمت فإنه في حالة حدوث خلل أو اختراق للنظام المحاسبي من خلال شبكة الانترنيت، تصبح مخرجات النظام المحاسبي مشكوكا بمصداقيتها وبالتالي، ستفقد ثقة المستخدمين .

ومما سبق نستطيع القول ، بأننا إن أردنا أن تكون معلومات النظام المحاسبي ذات موثوقية عالية جدا ، فانه لا بد من تحقيق أمرين مهمين: الأول: إيجاد آلية معينة لحماية النظام المحاسبي من الاختراقات عبر الانترنيت ، والثاني: إيجاد آلية معينة تؤكد على سلامة آلية التجارة الإلكترونية ومواقع تصفح الشركة في شبكة الانترنيت.

قد يبدو للوهلة الأولى أن ما يسعى إليه الباحثان هو عبارة عن أمور تكنولوجية بحتة ، لكن في حقيقة الأمر ، هو عبارة عن إجراءات رقابية محاسبية ذات طابع تكنولوجي يتماشى مع تغيرات التكنولوجيا العالمية والتي لا بد لعلم المحاسبة والتدقيق من مواكبتها .

سيحاول الباحثان تحقيق ثلاثة أمور رئيسية تساعد النظام المحاسبي المؤتمت للوصول إلى الدرجة الأقرب للمثالية في تحقيق الخصائص النوعية للمعلومات وبالتسلسل التالي :

1 -الأمان Security ، وهو عبارة عن اقتراح إجراءات تكنولوجية معينة تمنع الأخرين من اختراق النظام المحاسبي المؤتمت عبر موقع الشركة الإلكتروني على شبكة الانترنيت .

2 -التوكيدية Assurance ، وهي عبارة عن الآليات والإجراءات الواجب اتباعها لتأمين الحصول على نوعية معلومات جيدة، وقد عرفها معهد المحاسبين القانونيين الأمريكي AICPA على موقعه عبر الانترنيت وبشكل يتماشى مع مهنة التدقيق على النحو التالي:

" خدمات التوكيدية عبارة عن خدمات مهنية تحسن من نوعية المعلومات أو مداخلاتها والمرغوبة من قبل متخذي القرار"[1] .

3 -الموثوقية Reliability ، وهي عبارة عن الإجراءات الواجب اتباعها لجعل المعلومات موثوق بها من قبل أصحاب المصالح بشكل عام ومتخذي القرار بشكل خاص ، وإقناعهم بنجاعتها.

لقد اهتمت كثير من الهيئات المحاسبية العالمية وكذلك بعض الجامعات العريقة بموضوع التجارة الإلكترونية، وجعلت آلية السيطرة على العمليات المحاسبية التي تتم بواسطتها من لب اختصاص علم المحاسبة والتدقيق ، وعلى رأس تلك الهيئات ، معهد المحاسبين القانونيين الأمريكي AICPA والذي اقر خمسة مبادئ تدقيق لمواقع التجارة الإلكترونية للشركات في مشروعه المشترك مع معهد المحاسبين القانونيين الكندي CICA.

وكذلك اهتم معهد التدقيق الداخلي الأمريكي IIA بنفس الموضوع ولدرجة أنه أنشأ مجلة دورية باسم مجلة تدقيق تكنولوجيا المعلومات ، وأخذ يؤهل منتسبيه من محاسبين ومدققين بآليات تدقيق النظم المحاسبية المؤتمتة والتي تتعامل بالتجارة الإلكترونية .

ولقد ذكرت مجلة Business Wire في عددها الصادر في 2001/1/25 تحت عنوان " تتشارك هيئات المحاسبة العالمية بأفضل الممارسات التي تساعد أصحاب الأعمال على إدارة مخاطر التجارة الإلكترونية " . حيث ذكرت بأن معهد المحاسبين القانونيين الأمريكي وخمسة عشر معهدا محاسبيا محليا من أوروبا وجنوب أمريكا وأسيا قد اجتمعوا في سان فرانسيسكو لتقييم المخاطر التي ظهرت نتيجة التعامل بالتجارة الإلكترونية وبالأخص خطر الاختراقات والتعدي على الخصوصية ، ولقد أوضح Alan Anderson (نائب رئيس معهد المحاسبيين القانونيين الأمريكي) بأن عوائد التجارة الإلكترونية يتوقع أن تبلغ 6.4 تريليون دولار مطلع عام 2004[2]

---

[1] Assurance Services, The Opportunity That Exists for the Profession, (AICPA Web Site), https://aicpa.org/assurance .
[2] Global Accounting Profession Shares Best Practices to Help Businesses Manage E-commerce Risks, Business Wire, Jan. 25, 2001. , https://businesswire.com .

لكن هذا الرقم سيكون من الصعب تحقيقه بغياب مهنة تدقيق فاعلة على التعاملات الإلكترونية والتي إن وجدت ستقضي على فجوة الثقة (Trust Gap) وستؤمن للمتعاملين من الشركات بهذا النظام العالمي الجديد ثقة عالية جدا في تلك التعاملات .

وفي نهاية المقالة تم نصح الشركات والمهتمين بالاطلاع على آخر ما توصل إليه معهد المحاسبين القانونيين الأمريكي من ممارسات كفيلة بحصر فجوة الثقة عبر موقعهم المجاني على الانترنيت والممثل بالعنوان الإلكتروني www.aicpa.org/assurance/webtrust/princip.htm. ، وعند دخول الباحثان لهذا الموقع وجدا انه عبارة عن خدمة تدقيق جديدة يقدمها المعهد الى المتعاملين مع منتسبيه، تقوم فكرتها على تدقيق انظمة الشركات المتعاملة بالتجارة الالكترونية، ويستطيع الباحثان القول أن الموضوع الذي تدور الدراسة حوله موضوع محاسبي بحت مستندا على جميع الدلائل السابقة .

أثر التجارة الإلكترونية على كل من المحاسبة والتدقيق [1]

لقد أوضح (البرت مرسيلا Albert Marcella) في مقالته المعنونة بالتجارة الإلكترونية في مجلة تدقيق تكنولوجيا المعلومات الآثار التي تركتها التجارة الإلكترونية على كل من مهنة المحاسبة ومهنة التدقيق ، حيث أن هذه التكنولوجيا الحديثة أحدثت وتحدث تغيرات على كل من العناصر التالية :

1 - ممارسة المحاسب والمدقق.
2 - تقنيات المحاسب والمدقق.
3 - مهارات المحاسب والمدقق.
4 - معلومات المحاسب والمدقق.
5 - المعلومات الضرورية التي يجب أن يحيط بها كل من المحاسب والمدقق.
6 - التزامات المحاسب والمدقق.
7 - نوعية الخدمات المقدمة من قبل المحاسب والمدقق.

[1] Albert Marcella, Electronic Commerce, Opicit.

والنقطة المهمة والجدير ذكرها ، أن نظام الرقابة الداخلي تأثر وبشكل جوهري بوجود التجارة الإلكترونية ، حيث أصبحت الإجراءات الرقابية التقليدية عديمة الجدوى ، وأصبح لا بد من إجراءات رقابية تكنولوجية تواكب التغيرات التكنولوجية المصاحبة للتجارة الإلكترونية .

وأصبحت عملية التوكيد على نظام الرقابة الداخلي في ظل التجارة الإلكترونية من أكبر ، بل وأصعب التحديات التي تواجه كلا من المحاسب والمدقق.

وكما هو معروف بأن كلا من مهنة التدقيق والمحاسبة تعمل ضمن بيئة أعمال معينة ، ويبرز هنا سؤال مهم وملح ، ما هو دور كل من المحاسب والمدقق في حالة أن بيئة الأعمال قد تغيرت كليا ؟

التغيرات التي أحدثتها التجارة الإلكترونية في بيئة الأعمال

لقد أحدثت التجارة الإلكترونية تغيرات جوهرية في بيئة الأعمال التي يعمل بها كل من المحاسب والمدقق ، ويمكن تلخيص هذه التغيرات بالشكل التالي:

1 -هيكلية المنشأة Organization Structure ، لقد أحدثت التجارة الإلكترونية تغيرا جذريا على هيكلية المنشأة ، وجعلتها ذات طابع تكنولوجي بالكامل . فمن المعروف بأن عمليات المنشأة كانت تتم بشكل تقليدي في السابق، وعامل الوقت لم يكن ملحا كما هو الآن ، فعملية الشراء تتم بلحظات ، ولمواكبة السرعة الكبيرة لا بد أن تحوي هيكلية المنشأة الآليات الكفيلة التي تمكنها من ملاحقة العملية والتأكد منها وتنفيذها ، والذي يزيد الأمور صعوبة ، تعقيدات العمليات التي تتم من خلال شبكة الانترنيت ، وخصوصا في ظل الاختراقات الرهيبة التي يمكن أن يقوم بها قراصنة الانترنيت .

ولكي يواكب كل من المحاسب والمدقق هذه العمليات السريعة ، لا بد لكل منهما أن يتعلما هذه التكنولوجيا بشكل ممتاز وإلا أصبحا عديمي الجدوى .

2 -موقع الأعمال Location of the Business ، تعد هذه النقطة من أهم وأخطر التغيرات التي حدثت في ظل التجارة الإلكترونية ، فسابقا وبالنظام التقليدي كانت الأعمال تتداول في أماكن وأسواق محددة ، وفي حالة حدوث أي خطأ أو وروود

أي مشكلة كان من السهل الإحاطة بها وتداركها ، أما الآن وبواسطة التكنولوجيا العالية يستطيع أي شخص من أي مكان إتمام الجزء الأكبر من الصفقة بضغطة سريعة على لوحة مفاتيح جهاز الكمبيوتر ، وفي كثير من الأحيان تكون عملية تعقب العملية والشخص أشبه بالمستحيلة ، وخصوصا إن لم تكتشف المشكلة أو التلاعب في لحظة انتهاء العملية ، ومن الأمور التي تعاني منها الشركات المتعاملة بالتجارة الإلكترونية الاختراقات التي لا يتم اكتشافها إلا بعد فوات الأوان .

3 -قنوات التوزيع Distribution Channels ، ففي السابق كانت قنوات توزيع منتج الشركة (بيعه) محددة ومعروفة بشكل واضح وغير معقدة ، مما يمكن الشركة من تحديد مصدر العملية والتعامل معها بناءً على ذلك . ولكن وفي ظل التجارة الإلكترونية وتعدد أنواعها أصبحت قنوات التوزيع عديدة ومتشابكة ومعقدة ، وفي حالة حدوث أي خطأ ، قد ينقضي وقت كبير قبل إمكانية تحديد قناة التوزيع التي حصل فيها الخطأ .

4 -تعدد أشكال وسائط البيع Forms & Means of Sales ، وهذه تختلف نوعا ما عن قنوات التوزيع ، والمقصود هنا بأنه في السابق كانت وسائط البيع عبارة عن أشخاص مؤهلين لذلك ، ولكن الآن وبظل التجارة الإلكترونية أصبحت وسائط البيع عبارة عن برامج محوسبة وبأشكال متعددة ، منها الصوتية والمرئية وأنظمة كثيرة تقوم بعمليات البيع المبنية على برمجيات تم إعدادها مسبقا ، والمشكلة تكمن بأن جميع هذه البرمجيات لا تملك الحس والذكاء البشري وقد يستطيع الغير التلاعب بها .

5 -العلاقة مع الشركاء والزبائن Relationship with Partners & Customers ، وهذه تعد من النقاط المهمة جدا ، ففي الأسلوب التقليدي كانت العلاقة مع الشركاء والزبائن علاقة مباشرة ، ولكن الآن أصبحت العلاقة علاقة ذات طابع تكنولوجي رقمي ، وفي أغلب الأحيان العلاقة الشخصية معدومة ، وبالتالي أصبح التعامل أشبه بشكل ذي طابع وهمي رغم أنه حقيقة واقعة ولكن هذه الحقيقة قد يتم التلاعب بها بشكل لا يمكن تصوره .

6 -الاعتراف بالإيراد Revenue Recognition ، قد تعد هذه من أكثر المشاكل التي تؤرق المحاسب ، ويعتقد الباحثان بأن نظرية المحاسبة لم تأخذ بالحسبان آلية الاعتراف بالإيراد في ظل هذه الظروف التكنولوجية العالية . ففي السابق كان الاعتراف بالإيراد يتم وفقا لشروط محددة ، فتحقق الإيراد يمكن الجزم به في كثير من الأحيان، وكانت نقطة البيع مرتكزا لا يمكن تجاوزه إلا في بعض الحالات المحددة ، ولكن الآن وفي ظل غياب الأمان وإمكانية اختراق الشركة من قبل الغير جعل عملية تحقق الإيراد عملية مشكوك فيها .

ليس من السهولة البت بهذا الموضوع ، وفي رأي الباحثان إن استطعنا توفير الأمان للعمليات الإلكترونية واستطاع المحاسب المختص توكيد فاعلية الأمان ، يمكن بعدها التحقق من الإيراد .

وهذا يقود بالتالي إلى رغبة الباحثان باقتراح شروط جديدة لا بد من توافرها للاعتراف بالإيراد (الإلكتروني) ، إضافة للشروط المتعارف عليها والاقتراح هو ضرورة توفر كل من :

- الأمان في العمليات.
- توكيد آلية الأمان.

والتي سيتناولها الباحثان في نهاية الدراسة بالتفصيل.

7 -آلية التسديد Payment Processes ، في ظل التجارة الإلكترونية ظهرت آلية تسديد جديدة لم تكن موجودة سابقا ، وهي التسديد عبر شبكة الانترنيت . قد يظن البعض أن هذه الآلية لا تختلف كثيرا عن آلية التسديد عبر شبكات البنوك الإلكترونية ، ولكنها تختلف اختلافا جذريا ، فالبنوك تستخدم شبكات خاصة بها عبر نظم الاتصالات وهي شبكات محمية وغير متاحة للجمهور ، ولكن التسديد عبر شبكة الانترنيت محفوف بمخاطر كبيرة وعديدة وخصوصا عندما يتمكن قراصنة الانترنيت من استخدام حسابات الغير بتسديد مشترياتهم، وفي هذه الحالة يصبح من المستحيل إلغاء العملية، ويكون الخاسر الأول والأخير كل من الشركة البائعة والشخص الذي تم اختراق حسابه من غير علمه .

فلقد تعدى الأمر ضياع بطاقة اعتماد يمكن التعميم عليها وإيقافها ، إلى استخدام بطاقة اعتماد وحساب شخص بشكل لا يمكنه الشعور به إلا بعد فوات الأوان .

8 -احتساب ودفع الضرائب Tax Accounting & Payment ، ونعود مرة أخرى لمشكلة الاعتراف بالدخل ، فضريبة المبيعات أصبحت مشكلة تؤرق الشركات وخصوصا في ظل غياب الأمان على العمليات الإلكترونية ، فلقد أصبح من الصعب على الشركة إثبات التلاعب بدخلها وخصوصا أن أغلب الشركات لا تقر ولا تفصح عن وجود تلاعب خوفا من فقدان زبائنها، وبالتالي، قد تتحمل تكاليف إضافية وعلى رأسها الضرائب المفروضة على مبيعات قد تكون غير موجودة أصلا .

لكي يواكب كل من المحاسب والمدقق التغيرات الجوهرية في بيئة الأعمال الجديدة في ظل التجارة الإلكترونية ، أصبح لزاما عليهما الإلمام بالمعلومات والتقنيات الضرورية المصاحبة لهذا التقدم التكنولوجي الضخم ، ولكي يتمكنا من تقييم جميع تعاملات التجارة الإلكترونية والسيطرة عليها، أصبح لزاما عليهما الإلمام بالمفاهيم الحديثة المترابطة معها ، والتي يمكن تلخيصها بالآتي:

1 - التواقيع الإلكترونية الرقمية Digital/Electronic Signatures

2 - اتفاقيات تبادل البيانات Data Exchange Protocols

3 - عمليات الإلكترونية آمنة Secure Electronic Transactions

4 - الترخيص الإلكتروني Electronic Licensing

5 - البنية التحتية لمفاهيم الخصوصية والعمومية Public & Private Key Infrastructures

6 - رموز العمليات Token Transactions

7 - البطاقات الذكية Smart Cards

8 - النقد الإلكتروني Electronic Cash

9 - نقطة البيع Point of Sale

10 -أية أمور أخرى مستجدة

ويرى البعض[1] أن من أهم التغيرات التي أحدثتها التجارة الإلكترونية ، هو ظهور نوع جديد من الاقتصاد الذي تم تسميته (بالاقتصاد الرمزي) إلى جوار الاقتصاد العيني واقتصاد الخدمات .

التجارة الإلكترونية وعلاقتها بمعايير المحاسبة ومعايير التدقيق

في أواخر عام 1997 تنبهت هيئات المحاسبة والتدقيق المختصة لأهمية التجارة الإلكترونية وتوقعت أن تولد الأعمال الإلكترونية دخلا يتعدى التريليون دولار في نهاية عام 2002 وأصبحت مهنة المحاسبة من المهن الرائدة في تطوير معايير للتجارة الإلكترونية ، وذلك لتمكين منتسبيها من توفير التوكيدية بالتعامل بالتجارة الإلكترونية لبيئة الأعمال المتعامله بها [2].

وقد انشأ كل من معهد المحاسبين القانونيين الأمريكي وبالتعاون مع معهد القانونيين الكندي لجنة خاصة أوكلت إليها مهمة دراسة حاجة السوق لخدمات توكيد التعاملات بالتجارة الإلكترونية ، وذلك كي تتمكن كل من مهنة المحاسبة ومهنة التدقيق من الاستجابة السريعة لتلك الحاجات .

وقد تمكنت اللجنة فعلا من دراسة السوق ، وخلصت إلى أن المستهلكين قلقين من التعامل الإلكتروني ، ووجدت أن الأسئلة الرئيسية التي تتبادر إلى أذهانهم دوما هي :

1 - هل الشركة التي أتعامل معها عبر شبكة الانترنيت ، هي فعلا الشركة المعنية أم لا ؟

2 - هل في حالة أني زودت الشركة برقم بطاقة اعتمادي أو رقم حسابي ، تعد عملية آمنة ؟

3 - هل المعلومات الشخصية الخاصة بي لا يتم تداولها من قبل الغير في شبكة الانترنيت ؟

4 - هل سأتلقى طلبي نفسه الذي أطلبه عبر شبكة الانترنيت ؟

---

[1] زايري بلقاسم ودلوباشي علي ، مرجع سابق، صفحة (358).

[2] Appalraju Yogen, Accountants Chip in to Build Trust in E-commerce, Computing Canada, Nov. 23, 1998, Vol. 24, Issue 44, Page 28, https://ebscohost.com .

5 - هل سيتم الإيفاء بالتسليم وبالموعد المحدد ؟

6 - من الذي سيكفل حصولي على قيمة البضاعة المذكورة بموقع الشركة ؟

وانطلاقا من الأسئلة السابقة استطاعت تلك اللجنة إنشاء مشروع ما يسمي موثوقية الشبكة (Web Trust).

مخاطر التجارة الإلكترونية

تنبع مخاطر التجارة الإلكترونية ، وبشكل رئيسي من مخاطر شبكة الانترنيت فكل تكنولوجيا حديثه ورغم إيجابياتها الكثيرة إلا أن سلبياتها كثيرة كذلك وفي حالتنا هذه سلبياتها تعد خطيرة جدا ، وفي حالة عدم التمكن من تحجيم تلك السلبيات والسيطرة عليها ، ستكون النتائج مخيبة للآمال وقد يتم الإحجام عن هذه التكنولوجيا الحديثة، وبالتالي، تضييع أرباح وفوائد جمة .

وللأسف إن مخاطر التجارة الإلكترونية كثيرة ومتعددة ، وليس من السهل حصرها ، فتكنولوجيا التجارة الإلكترونية تكنولوجيا سريعة التغير والتطور وكل تغير أو تطور يواكبه مخاطر جديدة ، ويكمن الخطر الرئيسي في التجارة الإلكترونية في إمكانية اختراق الغير للمعلومات الخاصة لكل من المستهلك والتاجر.

ويذكر توم ارنولد Tom Arnold والمتخصص بتعقب عمليات الاختراق عبر شبكة الانترنيت[1] ، بأن عمليات الاختراق عبر التجارة الإلكترونية توقع الضرر الأكبر على التاجر أكثر منه على المستهلك (المشتري) ، فتعويض خسارة المشتري ممكنة، وخصوصا بأنه وبالغالب يستخدم بطاقات الاعتماد للدفع وتكون خسارته محددة بعملية واحدة ، والتي قد يمكن تعقبها ، ولكن الخسارة الحقيقية تقع على التاجر (الشركات) حيث تتكبد الشركة الخسائر بفقدانها الإيرادات والتي يصعب تعويضها أو حتى تعقب المتلاعبين بأنظمتهم المحاسبية ، وذلك نظرا لتعقيدات العمليات الكثيرة في التجارة الإلكترونية.

---

[1]Steve Hill, Safe Hands: Tom Arnold is the man corporates and even FBI call when they have a serious on line fraud problem. Steve Hill talks to him about the risks of e-commerce, identity scams and what we can all do to protect ourselves. (Internet Interview), Internet Magazine, March, 2002, https://findarticles.com .

ويرى المختص (توم ارنولد Tom Arnold) أن مخاطر التجارة الإلكترونية تصنف ضمن نوعين رئيسين وهما :

1 - مخاطر يمكن اكتشافها ، والمقصود هنا بأن الشركة وبوجود خبراء مختصين لديها قد تتمكن من اصطياد بعض الاختراقات في أنظمتها والتعامل معها ومن أشهر هذه الاختراقات :

- الفيروسات الرقمية المعروفة ، بوجود نظام حماية مناسب ، يستطيع نظام الشركة اصطياد هذه الفيروسات المعروفة له بشكل مسبق والقضاء عليها .

- قراصنة الانترنيت الهواة ، يعتمد قراصنة الانترنيت في اختراقاتهم لنظام الشركة على معلومات ورموز دخول معينة ، وفي حالة وجود أكثر من مستخدم لنظام الشركة قد يستطيع القرصان تتبع عملية الدخول والحصول من ذاكرة النظام على تلك المعلومات واستخدامها ؛ ولهذا فإن كانت الشركة تستخدم آلية تغير تلك الرموز بشكل دوري ومسح الذاكرة المعنية بواسطة خبرائها فستتمكن من تحجيم الاختراقات .

2 - مخاطر لا يمكن اكتشافها ، والمقصود هنا ، بأن بعض الاختراقات قد تتم دون سابق دراية بها ، إما لحداثتها أو جهل الشركة بها ، والنابعة من الأسباب التالية:

-فيروسات غير معروفة ، رغم وجود أنظمة حماية من الفيروسات على أنظمة الشركة ، إلا أنه هنالك فيروسات غير معروفة بعد للنظام قد تتمكن من دخول نظام الشبكة وإحداث تلف كبير دون الشعور به إلا بعد فوات الأوان ، كما حدث في عام 2000 عندما استطاع أحد الهواة اختراع فيروس I Love you ، والذي تمكن من إيقاع خسائر لم يمكن حصرها في ذلك الوقت ، ولقد كان الفيروس يعمل كقنبلة موقوتة ، حيث يفعل في تاريخ محدد بالسنة ، وكان الحل الوحيد لتفاديه بعد أن عرفت آلية عمله إغلاق النظام بالكامل في ذلك التاريخ .

-قراصنة انترنيت ذوي خبرة عالية ، وهذه تعد من أكبر المشاكل التي تواجهها الشركات ، فقراصنة الانترنيت ليسوا دوما من الهواة ، فبعضهم يملك خبرة ومهارة

تفوق كثيرا من المتخصصين ، تمكنهم وفي كثير من الأحيان من اختراق أنظمة الشركة دون أن يستشعر بهم ، وقد تتم جريمتهم دون اكتشافها .

- التسارع التكنولوجي ، قد يصعب في كثير من الأحيان مواكبة التسارع التكنولوجي على شبكة الانترنيت بشكل عام وعلى التجارة الإلكترونية بشكل خاص مما يجعل التكنولوجيا التي تستخدمها الشركة قديمة جدا ، والمشكلة تكمن بعدم معرفة التقادم في الوقت المناسب .

ويذكر معهد المحاسبين القانونيين الأمريكي على موقعه عبر الانترنيت ، أن بعض الدراسات أظهرت أن الخسائر التي تكبدتها الشركات الأمريكية في عام 1999 من اختراقات لبطاقات الائتمان فقط بلغت أربعمائة مليون دولار ويتوقع أن ترتفع سنويا إلى مبلغ ستين بليون دولار بحلول عام 2005 [1] ، ومن هذه الحقيقة يوضح المعهد الحاجة الملحة لإنشاء آلية حماية على الشبكة ، منطلقا من مخاطر التجارة الإلكترونية ، والتي تعزى للأسباب التالية :

1 - الهجمات المتعمدة Intentional Attacks ، والتي تتم إما بواسطة قراصنة الانترنيت ، أو منافسي الشركة لغرض الوصول إلى المعلومات السرية للشركة: كأرقام بطاقات اعتماد الزبائن مثلا والمعلومات السرية بالزبائن، وحجم المبيعات، وأمور كثيرة قد يصعب حصرها ، وحسب الغاية تكون الوسيلة .

2 - خصوصية التعامل The Privacy Debate ، تعتبر التعاملات الإلكترونية التي تتم بين الأفراد والشركة ذات طابع معلوماتي مهم جدا ، من منطلق أنها تحفظ على ذاكرة النظام الرقمية، وهي معلومات قيمة جدا ، وبالتالي إن تمكن أحد من معرفتها أو حتى تتبعها: مثل تتبع رقم بطاقة اعتماد العميل. ومن هنا سيشعر العميل بأن خصوصيته قد تم اختراقها وبالتالي سيفقد الثقة بالشركة التي تعامل معها من منطلق أنها لم تتمكن من حماية خصوصيته .

3 - فقدان الثقة Loss of Trust ، المقصود هنا فقدان ثقة الشركة بمعلومات عميلها ، فمن المتعارف عليه بأن العميل يستخدم ما يسمى التوقيع الرقمي Digital

[1] AICPA, What are Web Trust Services and Why Should I Get Involved? https://aicpa.org/assurance/webtrust/what.htm .

Signature الخاص به لدخول نظام الشركة لإتمام عمليته المرغوب فيها ، فكيف هو الحال إذا تمكن الشخص غير الصحيح بالدخول مستخدما توقيع العميل .

4 - فشل عملية التحويل Transmission Failures ، رغم أن عملية الشراء الإلكترونية تتم بسرعة كبيرة جدا ، إلا أنها عرضة لخطر فشل عملية التحويل فمن المتعارف عليه أن عملية الشراء عبر التجارة الإلكترونية تتم بواسطة عدة خطوات ، كأن يبدأ المستهلك بملء النموذج الابتدائي لعملية الشراء، ومن ثم الانتقال لنموذج ملء بيانات بطاقة الاعتماد، وخطوات أخرى قد تكون ضرورية وفقا لسياسات الشركة ، وفي كل مرحلة تفتح صفحة جديدة عبر موقع الشركة ولأسباب تقنية أو أخرى، قد تفشل إحدى الخطوات ، وهنا ستظهر مشكلة جديدة وهي عدم التأكد من إتمام العملية .

5 - غياب التوثيق Lack of Authentication ، ففي التجارة التقليدية يتم عادة توثيق الصفقة بأوراق ثبوتيه مروسة بشعار الشركة وموقعة من قبل الشخص المناسب، وبواسطة اتصال شخصي ومباشر بين البائع والمشتري ، ولكن في التجارة الإلكترونية تعد جميع تلك الأمور شبه مفقودة بالكامل ، وهذه الحقيقة تزيد من احتمالية التعامل مع الشخص غير الصحيح .

6 - سرقة الهوية Theft of Identity ، في غياب التوثيق المناسب كما في التجارة التقليدية يصبح من السهل على المجرمين انتحال شخصية الغير والقيام بالعمليات دون علمه .

7 - تزوير الحقائق Window Dressing ، ستكون خدمات بعض مسوقي ومزودي خدمات الحماية ، خدمات تجميليه فقط في غياب آلية معينة تؤكد مصداقيتهم وفاعلية خدماتهم .

8 - آثار ضغوط الاقتصاد Effects of Economic Pressures ، مع نمو التجارة الإلكترونية المتسارع ، أصبح سوقها سوقا تنافسيا ، وأصبحت قوة المتنافس الحقيقية تكمن في نجاح آليات الأمان والتوكيدية والموثوقية الخاصة بنظامه

المحاسبي ، وكل من يستطيع توفير تلك الآليات يكون نصيبه أكبر في هذا السوق التكنولوجي العالمي .

أسباب صعوبة تعقب الاختراقات التي تتم عبر شبكة الانترنيت

يعد نظام التجارة الإلكترونية بيئة مثالية للسرقات والتلاعب وإخفاء آثار الجريمة بشكل متقن منقطع النظير ، ويعود السبب في ذلك للعوامل التالية :

1 - إمكانية الدخول من عدة أماكن ، فالمتعامل عبر الانترنيت لا يحتاج إلى مكان محدد لدخول الشبكة ، فأي شخص يمكنه الدخول إلى الشبكة من أي مكان يتوفر به جهاز كمبيوتر وخط اتصال ، كمقاهي الانترنيت ومختبرات الجامعات والمدارس.

2 - سرعة العملية ، قد لا يحتاج الدخيل (المخترق) إلى أكثر من بضع دقائق لاختراق موقع معين والتلاعب به ومغادرة الموقع قبل أن يتم تعقبه.

3 - تباعد المسافات ، قد يكون المخترق لموقع ما يبعد آلاف الكيلومترات وفي بلد آخر ، فشبكة الانترنيت صممت بشكل عالمي .

4 - عدم وجود هوية محددة ، لا يمكن معرفة ماهية المخترق ولا بأي شكل من الأشكال .

5 - عدم وجود قوانين دولية ، فشبكة الانترنيت شبكة عالمية ذات معايير موحدة بالاستخدام فقط ، ولو أننا افترضنا اكتشاف أحد المخترقين بدولة مغايرة لدولة الشركة التي تم اختراقها ، فإنه ليس بالضرورة وجود قوانين موحدة للتعامل مع المخترق .

6 - عدم وجود دلائل مادية ، لإثبات أي جريمة لا بد من توفر دلائل وقرائن مادية ولكن أين هي هذه الدلائل في هذه الشبكة المرئية فقط؟

7 - إمكانية إتلاف بيانات جهاز الكمبيوتر ، في حالة شعور أي مخترق بإمكانية تعقبه يستطيع إتلاف بيانات جهازه بضغطة زر بسيطة ، مما يجعل عملية تعقبه عديمة الجدوى .

8 - حماية الحسابات البنكية ، هناك الكثير من الحسابات البنكية محمية من اطلاع الغير عليها ، وبالتالي يستطيع المخترق استخدام هذا النوع من الحسابات دون القلق من آلية تعقبه .

9 - عدم الإبلاغ عن الاختراقات ، هناك الكثير من الشركات لا تبلغ عن الاختراقات التي تعرضت لها أنظمتها ؛ خوفا من فقدان عملائها وتفضل تحمل خسائر كبيرة عوضا عن فقدان الثقة بها ، وخير دليل على ذلك عملية الاختراق التي تمت لبنك City Bank في مطلع عام 2001 من قبل شخص بروسيا كبدته خسائر قدرت بعشرة ملايين دولار والتي *لغاية هذه اللحظة* ترفض الإقرار بها .

الحلول المقترحة للسيطرة على مخاطر التجارة الإلكترونية

لقد حاولت عدة جهات اقتراح الكثير من الخطوات لمواجهة مخاطر التجارة الإلكترونية ، وقد كان معهد المحاسبين القانونيين الأمريكي من أولى الجهات التي قدمت اقتراحات قيمة في الاجتماع الذي عقد في مدينة باريس في الأول من أغسطس لعام 2000 ، والذي ضم عدة جهات محاسبية مهنية متخصصة بهدف إيجاد حلول لمخاطر التجارة الإلكترونية التي يواجهها المستهلك، ويمكن تلخيص هذه المقترحات على الشكل التالي[1] :

1- توخي الحذر بإعطاء المعلومات الشخصية ، وذلك بعدم إعطاء المعلومات الشخصية ، إلا للجهات الموثوق بها ، ومعرفة أسباب حاجة تلك الجهات لهذه المعلومات ، وتتضمن المعلومات الشخصية بشكل أساسي كلا من العنوان البريدي وأرقام الهواتف والبريد الإلكتروني.

2- استخدام برنامج آمن للدخول إلى شبكة الانترنيت ، من المعروف أن كل جهاز كمبيوتر يحتوي على برنامج خاص للدخول إلى شبكة الانترنيت وفي الغالب، فإن هذه البرامج تحتوي على آليات معينة تحفظ في ذاكرة الجهاز جميع المعلومات التي تم تداولها في الشبكة من خلاله.

[1] AICPA Joins Global Accounting Profession in Paris to Explore Solutions to E-commerce Risks; Group Recommends Top 10 Ways to Protect Online Privacy, Business Wire, Aug. 1, 2000. , https://businesswire.com .

وفي كثير من الأحيان يستطيع المخترق وعبر الانترنيت الدخول لذاكرة هذا البرنامج والحصول على جميع المعلومات الخاصة بالمستخدم ودون أن يستشعر بذلك ولهذا ينصح بشراء برنامج خاص يتمتع بحماية عالية لمنع المخترق من الدخول إلى ذاكرته .

3- التأكد من موقع التاجر على الشبكة ، يجب التأكد بأن الموقع الخاص بالتاجر هو الموقع المقصود ، وذلك بالاطلاع على سياسات التاجر والتي تتضمن الموقع الأم والذي تم إنشاء موقع التاجر من خلاله . كما انه يمكن معرفة موقع التاجر من خلال آلية التصفح الخاصة Uniform Resource Locator (URL) من منطلق أن هذه الآلية تمكن من تتبع الموقع ومعرفة أسس إنشائه ، وفي حالة عدم التمكن من تتبعه فيكون الموقع في الغالب موقعا مشكوكا به .

4- استخدام بطاقات الدفع المضمونة ، يفضل استخدام بطاقات دفع مضمونة أو محمية ، والمقصود بذلك أن يتم التعامل مع مصدري بطاقات الدفع عبر الانترنيت والذين يتمتعون بسياسات خاصة تحمي الشخص المتعامل من مسؤولية الاستخدام غير المرخص لبطاقته من قبل الغير .

5- الحذر من تنزيل برامج عبر الانترنيت غير موثوقة المصدر ، من المعروف أن مستخدم الانترنيت وعبر تجوله بالشبكة ضمن مواقع متعددة يستطيع تنزيل برامج مجانية على جهازه ، يتم استخدامها لأغراض كثيرة: مثل برامج العرض الصوتية والمرئية وأغراض كثيرة . يجب توخي الحذر الشديد عند تنزيل تلك البرامج وخصوصا من المواقع المشكوك بأمرها ، لأنها قد تكون مبرمجة بآلية معينه تقوم على تجميع كل الأمور الخاصة بك والموجودة على جهازك وترحيلها للجهة المنشئة للبرنامج وذلك دون شعورك بذلك .

6- الحذر من إعطاء أرقامك السرية ، ويشمل هذا التحذير كل أرقامك السرية وبشتى أشكالها وأنواعها ، وخصوصا الأرقام الخاصة بدخولك للشبكة عبر مزود الخدمة . كما ينصح كذلك وعند إنشاء أرقامك السرية أن تبتعد عن الأمور التقليدية بإنشاء الرقم ، كأن تستخدم اسمك أو رقم هاتفك ، ويفضل أن تجعل

رقمك السري معقدا نوعا ما وتضمنه مجموعة من الأرقام والأحرف والرموز وكلما كان رقمك السري معقدا ، كان اكتشافه صعبا . فمن المعروف أن قراصنة الانترنيت استطاعوا وبشكل مذهل إنشاء برامج تكنولوجية ، والتي تعمل بنظام الاحتمالات ، تستطيع حل شفرة الأرقام السرية وبسرعة خيالية ، ولكنها قد تعجز عن ذلك ، فكلما كان الرقم معقد التكوين ومتضمناً لرموز وأرقام وأحرف كانت مقدرة تلك البرامج على فك تشفيره ضئيلة جدا.

7- الاحتفاظ بنسخ من العمليات ، وهذه تعد من الأمور المهمة والتي تساهم في اكتشاف السرقات وتفادي استمرارها . والمقصود بأن تحتفظ دوما بنسخة من عملية الشراء التي قمت بها (كمستهلك) عبر شبكة الانترنيت ، وكذلك بالاستمرار بعمل تسويات الشراء مع مصدر بطاقة الدفع . والمقصود هنا أمران مهمان جدا وهما :

- الاحتفاظ بنسخة من طلب الشراء ورقم الطلبية ، وهذا سيساعدك على الاتصال مع التاجر لحل إشكاليات عدة ، كموعد التسليم ومطابقة الطلبية وبالتالي تحييد الآخرين من الاستخدامات غير المرغوب فيها .

- الاستمرار بتسوية حسابات الدفع ، ويفضل أن تكون مطابقتك لحسابات الدفع عبر الانترنيت تسوية ذات طابع زمني قصير ، وذلك لاكتشاف الاختراقات بوقت سريع وإيقاف آلية الدفع عند الضرورة ؛ لكي لا يستطيع المخترق الاستمرار باستخدام بطاقتك .

8- راقب استخدام الموقع للمحددات Cookies ، والمحددات Cookies هي: عبارة عن رموز رقمية تساعدك بدخول الموقع دون إعادة كتابة رقمك السري وعادة ما يتم إدخالها إلى جهازك من قبل الموقع دون طلب الإذن منك بذلك ، وآلية عمل هذه المحددات بأنه وعند دخول الموقع مرة أخرى ، يقوم الموقع بالاتصال بتلك المحددات والموجودة على جهازك ومطابقتها برقمك السري ومن ثم السماح له بالدخول دون طلب الرقم السري . وفي الغالب يستطيع قراصنة الانترنيت تتبع هذه

المحددات Cookies على جهازك عندما تكون على الشبكة ، ولذلك يفضل برمجة جهازك على طلب الإذن منك قبل أن ينزل الموقع تلك المحددات عليه .

9- عدم السماح للأطفال باستخدام الشبكة دون إشراف ، تأكد بأنك تشرف على أطفالك عندما يستخدمون الانترنيت ، خصوصا أنهم يستطيعون إعطاء جميع المعلومات الشخصية عن حسن نية ، والتي تكون كفيلة بتمكين الغير من اختراق جهازك وبكل سهولة .

10- استخدم المواقع المرخصة ، والمقصود بالمواقع المرخصة ، تلك المواقع التي تم تقييمها وتأهيلها من قبل طرف ثالث مؤهل بأمور الحماية ، حيث أن ذلك النوع من المواقع يكون ممهورا بتوقيع إلكتروني خاص من طرف ثالث مهني متخصص كمعهد المحاسبين القانونيين الأمريكي .

من الملاحظ أن أمور الحماية العشرة السابقة والتي ينصح باتباعها من قبل معهد المحاسبين القانونيين الأمريكي ، هي أمور حماية خاصة بالمستهلك ، والسبب بذلك أن التاجر يستطيع توفير آليات حماية عديدة والتي قد تكون باهظة الثمن ، ولكن المستهلك لا يستطيع ذلك . وبالطبع يعتبر المستهلك حجر الأساس في التعامل الإلكتروني ، وفي حالة فقدانه الثقة لهذا النوع من التعامل ستكون التكنولوجيا هذه عديمة الجدوى .

وكنظرة اقتصادية ناجحة ، فان توفير الخدمات والنصائح المجانية للمستهلك ستشجعه على التعامل عبر التجارة الإلكترونية ، وبالتالي تأمين إيرادات خيالية لكل من التاجر والمؤسسات المهنية الخاصة . ولو أمعنا النظر بالاقتراح العاشر استخدام مواقع مرخصة ، سنجد اليوم بأن الكثير من الهيئات المهنية المحاسبية وعلى رأسها معهد المحاسبيين القانونيين الأمريكي ،تمارس خدمة جديدة تسمى موثوقية مواقع الشبكة العنكبوتية عبر الانترنيت Web Trust ، وهذه الخدمة كفيلة بتوفير إيرادات خيالية معتمدة على إيرادات المتاجرين عبر التجارة الإلكترونية . والجدول

التالي يوضح مبالغ الإيرادات عبر التجارة الإلكترونية لعام 1997 بالولايات المتحدة الأمريكية[1] :

إيرادات السلع		إيرادات الخدمات	
الألبسة	46 مليون دولار	اللهو	85 مليون دولار
الهدايا	15 مليون دولار	اشتراكات	120 مليون دولار
كتب	16 مليون دولار	خدمات بالغين(جنس)	52 مليون دولار
مواد غذائية	39 مليون دولار	موسيقى	9 ملاين دولار
سلع أخرى	37 مليون دولار	خدمات مالية	68 مليون دولار
		خدمات تأمين	39 مليون دولار
مجموع السلع	153 مليون دولار	مجموع الخدمات	373 مليون دولار

ومن الملاحظ وبعد أن تنبهت المعاهد المحاسبية المهنية لأهمية التجارة الإلكترونية قامت بالحث على إيجاد آليات ومعايير محاسبية خاصة لحماية التعاملات عبر الانترنيت بواسطة التجارة الإلكترونية ، ووجود هذه الآليات والمعايير مكنت الشركات بشكل أو بآخر من كسب ثقة المستهلك بالتعامل معها عبر هذه الآلية التكنولوجية الحديثة . وبعض الإحصائيات عكست هذه الثقة المتولدة بمساعدة الهيئات المحاسبية المهنية .

لقد أشارت الدراسة التي أجرتها شركة Forrrester Research Cambridge [2] بأنها تتوقع بأن حجم المبيعات عبر الانترنيت في الولايات المتحدة الأمريكية وحدها سوف يصل إلى 269 مليار دولار بحلول عام 2005 ، وهذه زيادة هائلة إذا ما قورنت مع حجم مبيعات عام 2000 والذي بلغ 44.8 مليار دولار . وتشير الشركة صاحبة

[1] زايري بلقاسم ودلوباشي علي ، مرجع سابق، صفحة (366)

[2] طاهر محسن الغالبي وأحمد شاكر العسكري ، تحديات التجارة الإلكترونية والعولمة ، المؤتمر العلمي السنوي الثاني لتكنولوجيا المعلومات ودورها في التنمية الاقتصادية ، كلية الاقتصاد والعلوم الإدارية ، جامعة الزيتونة 6-8 أيار _مايو) 2002 ، صفحة رقم 186 .

الدراسة أن التوقعات في زيادة عمليات الشراء والبيع من قبل بعض الصناعات الأمريكية بين عامي 2000 و 2005 ستكون على الشكل التالي:

الزيادات في التعامل عبر الانترنيت في بعض الصناعات الأمريكية (مليار دولار)

الصناعة	عام 2000	توقعات عام 2005
الغذائية والمشروبات	35	863
المعدات الصناعية	20	565
الحاسوب والاتصالات	90	1028
السيارات وقطع الغيار	21	660
الإنشاءات والعقارات	19	528

ويستطيع الباحثان القول بأن الثقة التي ولدتها الجهات المحاسبية المهنية المتخصصة بالتجارة الإلكترونية جعلت إيرادات الشركات ترتفع بشكل خيالي عبر التعامل من خلال التجارة الإلكترونية ، ولم يكن من الممكن أن تحقق الشركات تلك الإيرادات الخيالية دون جهود تلك الجهات المحاسبية المهنية. لقد أصبح هذا السوق الجديد ، ورغم مخاطره العديدة ، سوق العصر وسوق العولمة والتنافس المنقطع النظير ، علما بأن آليات التعامل فيه تختلف كليا ، بل جذريا عن آليات التعامل المتبعة بالسوق التقليدي .

الفرق بين التجارة الإلكترونية والتجارة التقليدية

مما سبق نستطيع ملاحظة الفرق بين التجارة الإلكترونية والتجارة التقليدية وخصوصا عندما تطرقنا لبيئة العمل في كل منهما .

ومن وجهة نظر محاسبية بحتة ، فإن عملية البيع والشراء تعد جوهر الاختلاف فيما بين التجارة الإلكترونية والتجارة التقليدية ، فالإجراءات الرقابية المتبعة في كل من البيئتين مختلفة تماما ، والاختلاف الرئيسي يمكن حصره بالقول

إن التجارة التقليدية ذات طابع توثيقي ، بينما التجارة الإلكترونية ذات طابع غير توثيقي (وهمي) ، رغم حقيقة تمام العملية .

ويمكن معرفة الفرق بشكل أعمق ، بعمل مقارنة بسيطة بين دورة البيع في كل من التجارة الإلكترونية والتجارة التقليدية ، وبالشكل التالي[1] :

مرحلة دورة المبيعات	التجارة التقليدية	التجارة الإلكترونية
البحث عن معلومات منتج	مجلات وممثل تجاري	صفحة Web
طلب المنتج	رسالة أو وثيقة	بريد إلكتروني
التأكيد على الطلبية	رسالة أو وثيقة	بريد إلكتروني
مراقبة السعر	كتالوج مطبوع	كتالوج على Web
التأكد من توفر السلعة	هاتف أو فاكس	لا يوجد
تسليم الطلبية	وثيقة مطبوعة	بريد إلكتروني
بعث الطلبية	فاكس أو بريد	بريد إلكتروني
التأكد من توفر السلعة بالمخازن	وثيقة مطبوعة	قاعدة بيانات
تخطيط التسليم	وثيقة مطبوعة	قاعدة بيانات
تعميم الفاتورة	وثيقة مطبوعة	قاعدة بيانات
تسلم السلعة	المورد	
تأكيد التسليم	وثيقة مطبوعة	بريد إلكتروني
بعث الفاتورة	بريد عادي	بريد إلكتروني
مدة الدفع	وثيقة مطبوعة	قاعدة بيانات
بعث التسوية المالية	بريد عادي	قاعدة بيانات

يلاحظ من جدول المقارنة السابق ، بأن التجارة الإلكترونية تفقد عامل التوثيق في أغلب المراحل ، وغياب التوثيق له دور سلبي جدا على آلية الاعتراف بالإيراد وخصوصا أن أغلب العمليات ذات طابع غير ملموس.

[1] زايري بلقاسم ودلوباشي علي ، مرجع سابق، صفحة (361) .

ويعتقد الباحثان بأن غياب التوثيق وترافقه مع مخاطر التجارة الإلكترونية له أثر مباشر على أساس أو قاعدة العمليات ، ويساهم بمشكلة جديدة متعلقة بعملية تحقق الإيراد والاعتراف به.

فتحت عنوان الاعتراف بالإيراد وتحققه ، أوصت لجنة المحاسبة الأمريكية عام 1964 بأنه يمكن تحسين مفهوم التحقق إذا طبقت المقاييس التالية[1] :

1 - يجب أن يكون الإيراد قابلا للقياس.

2 - يجب أن يدعم صحة التحقق قياس نتيجة حدوث عملية تبادلية مع أطراف خارجية.

3 - يجب حدوث الحدث الحاسم وهو بأن الإيراد يجب أن يتحقق عند إتمام معظم العمل أو المهمة في عملية الاكتساب . وينتج عن هذا الاختبار الاعتراف بالإيراد في أوقات مختلفة لمنظمات الأعمال المختلفة.

"أن استعمال مفهوم أو معيار "التحقق" عادة ما ينتج عنه الاعتراف بالايراد عند نقطة البيع ، ومع ذلك ، فإن توقيت الاعتراف قد يكون مسبقا أو يتم تأخيره حسب طبيعة العملية وبالنظر لدرجات التأكد المختلفة . فعندما يكون هناك درجة عالية من التأكد مرتبطة مع تحقق الإيراد ، فإن الاعتراف بالإيراد قد يسبق نقطة البيع وعلى العكس من ذلك ، كلما كانت درجة عدم التأكد عالية بالنسبة لارتباطها بتحقق الإيراد ، زاد الاتجاه بصورة أكبر لتأخير الاعتراف بالإيراد"[2].

من الجدير بالذكر ، أن معايير المحاسبة وضعت أسسا لمعالجة عملية الاعتراف بالإيراد في ظل ظروف عديدة ، ولكن ضمن التجارة التقليدية الموثقة ، ولكنها لم تضع أسسا خاصة لمعالجة الاعتراف بالإيراد في ظل التجارة الإلكترونية غير الموثقة.

تحت ظروف خاصة للاعتراف بالإيراد ، ذكر المعيار المحاسبي الأمريكي رقم SFAS No. 48 [3]تحت عنوان "الاعتراف بالإيراد عند وجود حق رد السلعة" أن على البائع

---

[1]Richard G. Schroeder; Myrtle W. Glark; & Jack M. Cathey, Accounting Theory and Analysis, 7th Edition, John Wiley & Sons, Inc. 2001, Page (72).

[2]Richard G. Schroeder, Ibid., P. (72) .

[3]Ibid., P. (74) .

الاعتراف بالإيراد عند نقطة البيع عندما يوجد حق الرد فقط حين تلبى الشروط التالية:

1 - أن يكون سعر البيع محددا أو ثابتا بتاريخ البيع.

2 - أن يكون المشتري قد دفع أو ملتزما بالدفع للبائع.

3 - أن يتحمل المشتري مخاطرة الخسائر نتيجة السرقة أو تلف البضاعة.

4 - أن يكون الجوهر الاقتصادي للمشتري بعيدا كل البعد عن الجوهر الاقتصادي للبائع .

5 - أن لا يكون للبائع التزامات رئيسية للأداء المستقبلي بالنسبة لإعادة بيع السلعة.

6 - إمكانية التقدير المعقول للمردودات المستقبلية.

وفي حالة عدم تلبية هذه الشروط ، يتوجب تأجيل الاعتراف الى أول نقطة يكون عندها قد انتهى حق الإرجاع .

وقد ذكرت نشرة لجنة الأوراق المالية الأمريكية SEC رقم SAB No. 101 ، بأنه لا يجوز الاعتراف بالإيراد إلا إذا تحقق أو هنالك إمكانية لتحققه ، وتم اكتسابه وفقا للمعايير التالية[1]:

1 - وجود دلائل مقنعة بالإثبات.

2 - تحديد سعر البيع من قبل البائع للمشتري .

3 - تم تسليم البضاعة أو تمت تأدية الخدمة .

4 - عملية التحصيل مؤمنة بشكل معقول .

ويستطيع الباحثان القول بأن الإيراد المتولد عبر قنوات التجارة الإلكترونية لا يتماشى مع بعض من شروط الاعتراف بالإيراد . فالمعيار الأمريكي رقم 48 وضمن الشرط رقم (2) " أن يكون المشتري قد دفع أو ملتزما بالدفع للبائع" يجعل الاعتراف بالإيراد عند نقطة البيع مستحيلا ، والسبب أن عملية الدفع ضمن آلية

[1]Ibid., P. (75) .

التجارة الإلكترونية ، آلية محفوفة بالمخاطر وقد تكون إذا ما تم التلاعب بها عملية وهمية ويقابلها خروج حقيقي للبضائع من عند التاجر . لو أردنا استخدام الاعتراف بالإيراد عند وصول النقد بدلا من نقطة البيع لما أمكن ذلك، والسبب بأن النقد وفي حالة التلاعب لن يصل ، ولا بد أن نتذكر أن التلاعب لم ينجم عن إدارة الشركة بل عن جهة خارجية غير معروفة .

وبالنسبة للشرط رقم (3) وفي نفس المعيار "أن يتحمل المشتري مخاطرة الخسائر نتيجة السرقة أو تلف البضاعة" ، وفي حالة التلاعب ، فمن هو المشتري؟ لا أحد يعرف والمتحمل الأول والأخير لهذه الخسارة هو الشركة البائعة ، وهنا يتبادر للذهن ، ما هي الآلية المناسبة للاعتراف إذن؟

ولو نظرنا لنشرة الأوراق المالية رقم 101 والمستندة على معايير المحاسبة الأمريكية لوجدنا أن كلا من المعيار رقم (1) "وجود دلائل مقنعة بالآليات" والمعيار رقم (4) "عملية التحصيل مؤمنة بشكل معقول" ، مفقودان بشكل شبه كامل في الإيرادات المتولدة من خلال التجارة الإلكترونية .

وفي ظل هذه الحقائق الجديدة يرغب الباحثان في اقتراح آلية جديدة أو نقطة جديدة للاعتراف بالإيراد المتولد من خلال التعامل بالتجارة الإلكترونية والتي يرغبان بتسميتها (الاعتراف بإيراد التجارة الإلكترونية عند نقطة تحقق أمان عمليات النظام E-commerce Revenue Recognized as System Transactions are Secured) .

يتضمن هذا الاقتراح ، أن يتم الاعتراف بالإيراد المتولد عبر التجارة الإلكترونية عند نقطة البيع ، إذا ما توفرت شروط إضافية تساعد على تحقيق الشرط رقم (2) " أن يكون المشتري قد دفع أو ملتزما بالدفع للبائع" في المعيار رقم 48 ، وبالشكل التالي:

1 - الأمان في العمليات Transaction Security
2 - توكيد آلية الأمان Assuring Security Process

وكل شرط يجب أن يصاحبه عدد من الآليات والمحددات ، وبالشكل التالي :

الأمان في العمليات Transaction Security ، ويقصد هنا بأنه يجب على الشركة تطوير نظام ربط بين نظام الشركة المحاسبي وموقعها على الانترنيت يضفي صفة الآمان على عمليات البيع التي تتم من خلاله ، متضمنا سياسات يتم برمجتها تؤمن كلا من:

1 -الأمان.

2 -التوكيدية.

3 -الموثوقية.

توكيد آلية الأمان Assuring Security Process ، حيث يتم ذلك بواسطة اعتماد إحدى الجهات المحاسبية المتخصصة ، بتدقيق نظام الشركة الخاص والذي يربط بين نظام الشركة المحاسبي وموقعها على الانترنيت ، كطرف ثالث محايد ، والذي يستطيع التأكيد على سلامة وصحة الإجراءات والسياسات المتبعة في ذلك النظام .

وأخيرا وليس آخرا ، وفي حالة تمكننا من الاعتراف بالإيراد المتولد من خلال التعامل بالتجارة الإلكترونية ستتمكن الشركة من تقدير نسبة الاحتيال عبر التجارة الإلكترونية E-commerce Frauds are Reasonably Estimable ومن ثم التمكن من إنشاء مخصصات معينة ، تقابل الخسائر المتوقعة مستقبليا والتي سيمكن توقعها بسهولة ، في ظل توافر الشروط السابقة .

ويمكن القول بأن التجارة الإلكترونية ، وكما أحدثت من تغيرات كثيرة على عالم الأعمال والاقتصاد ، أحدثت وستحدث تغيرات أكثر وأكبر على عالم المحاسبة وعالم التدقيق .

ففي السابق كانت التغيرات التي تحدث في ظل التجارة التقليدية ، تغيرات ذات طابع بسيط وبطيء ، وكان يسهل على كل من مهنة الأعمال ومهنة المحاسبة مواكبتها ؛ ولكن الآن، وفي ظل التجارة الإلكترونية وما يرافقها من تقنيات تكنولوجية عالية ومتغيرة بشكل متسارع أصبحت التغيرات في التجارة الإلكترونية ذات

طابع معقد جدا وسريع ، وأصبح محتوما على مهنة الأعمال ومهنة المحاسبة وفي العالم ككل أن تحدث وتطور من تقنياتها وتقييمها بسرعة مماثلة كي لا يفوتها الركب التكنولوجي الجديد .

المراجع

•ابو الليل ،إبراهيم دسوقي .البيع بالتقسيط والبيوع الائتمانية الأخرى .الطبعة الأولى الكويت: مطبوعات جامعة الكويت. 1404هـ -1984م.

•التركي، سليمان تركي سليمان. بيع التقسيط وإحكامه . رسالة ماجستير. قسم الفقه –كلية الشريعة، جامعة الإمام محمد بن سعود الإسلامية، الرياض:جمادى الأولى 1416هـ.

•الخضري ،ليلى محمد إبراهيم ،وآخرون."الاتجاهات الحديثة في علوم الأسرة (الاقتصاد المنزلي) .الطبعة الأولى . دار القلم للنشر والتوزيع .دبي.1420هـ. 1999م .

•القرني، عبد الرحمن. "التقسيط المريح...ورطة أصحاب الدخل المحدود " .صحيفة عكاظ .(العدد12983 -السنة الرابعة والأربعين . الخميس 30ذو الحجة 1422هـ -14 مارس 2002م).

• -باصبرين ،سكينة محمد عبد الرحمن. "إدارة المرأة العاملة لبعض موارد أسرتها في جدة". رسالة ماجستير. قسم اقتصاد منزلي . كلية التربية للبنات بجدة:1407هـ 1967هـ

•باصبرين ،سكينة محمد عبد الرحمن ."تخطيط الإنفاق على تأثيث المسكن الحديث في جدة وعلاقة ذلك بالنواحي الاقتصادية والجمالية".رسالة دكتوراه. قسم اقتصاد منزلي . كلية التربية للبنات بجدة1413هـ . 1993م .

•بيومي، ناهد يوسف."سياسة البيع بالتقسيط للسلع المعمرة مع دراسة ميدانية في بعض الوحدات الاقتصادية في جمهورية مصر العربية ". رسالة ماجستير في.قسم إدارة الأعمال –كلية التجارة. جامعة الإسكندرية، الإسكندرية:1979م.

• -باصبرين ،سكينة محمد عبد الرحمن ،" ترشيد استهلاك الطاقة الكهربائية للأسرة السعودية" .المؤتمر المصري للاقتصاد المنزلي .جامعة المنوفية .مصر.24 -25مارس 1996م .

• -باصبرين ، سكينة محمد عبد الرحمن ."دراسة لأنماط إنفاق مصروف طفل المرحلة الابتدائية ".مجلة المنصورة للعلوم الزراعية .مجلد23.العدد 7.جامعة المنصورة. كلية الزراعة .مصر.1998م.

- 10. -باصبرين ، سكينة محمد عبد الرحمن ."تخطيط الدخل المالي للأسرة السعودية مستخدمة البطاقة الائتمانية" .مجلة الإسكندرية للبحوث الزراعية ،جامعة الإسكندرية ،ابريل 200م.
- 11. -حقي، زينب محمد."الإدارة ومتغيرات العصر بين النظرية والتطبيق في مجالات الحياة الإنسانية" .مكتبة عين شمس . القاهرة.200م .
- 12 -حنا، بول. "المحفز المالي،نصائح سريعة للنجاح في معاملاتك المالية "الطبعة الأولى .جدة . مكتبة جرير.2003.
- 13. - خلاف، احمد اسعد. "الاثار التسويقية لسياسة البيع بالتقسيط _ دراسة ميدانية في وكالات السيارات اليابانية في مدينة جدة" . رسالة ماجستير. كلية الاقتصاد والإدارة_جامعة الملك عبد العزيز ،جدة : 1412هـ - 1992م .
- 14. - رزق الله ،عايدة نخلة. "تقييم نشاط البيع بالتقسيط في سوق المستهلك النهائي " . رسالة ماجستير. كلية التجارة - جامعة عين شمس القاهرة : 1975م .
- 15. -نور،سهير محمد فؤاد ،وآخرون "الاقتصاد الاستهلاكي الأسري " . قسم الاقتصاد المنزلي ،كليه الزراعة ،جامعة الإسكندرية ،1994م .
- 16. -عبد الجواد، محمد احمد."قد سفينتك في الإتجاه الصحيح ".الطبعة الأولى.جدة. دار الأندلس الخضراء:1424هـ.
- 17. - كوجك ،كوثر حسين . الإدارة المنزلية.الطبعة التاسعة.القاهرة:عالم الكتب.1997.هـ.2005م .
- 18. -سعيد، سلوى احمد.52ثالمالك، حصة صالح"إدارة موارد الأسرة اقتصادياتها...وترشيد استهلاكها".دار الزهراء.الرياض .1426.
- 19. - مزاهره ، أيمن سليمان .وآخرون ."اقتصاديات الأسرة : إدارة المنزل " . الطبعة الأولى.قسم الاقتصاد المنزلي .كلية الأميرة عالية الجامعية .جامعة البلقاء التطبيقية.2002م.
- 20. - مجلة الاقتصاد الإسلامي .من قرارات مجلس مجمع الفقه الإسلامي في مؤتمرة السادس المنعقد في جدة. (العدد 134 -السنة الثانية عشر - محرم:1413هـ -يوليو 1998م.

- مجلة الاقتصاد والنفط ."سوق البيع الآجل في السعودية تتجه إلى التنظيم والبلورة " .العدد 124 - السنة11 -1414هـ -ديسمبر :1994م.
- ملة، رفعة بنت تركي إسماعيل."أثرا لشراء بالتقسيط على أدارة المورد ة المالي للأسرة السعودية".رسالة ماجستير .قسم السكن وأداره المنزل. كلية التربية للاقتصاد المنزلي والتربية الفنية بجدة:1425هـ.2004 23 - موسى، -23 - منى حامد إبراهيم حامد."أثر استخدام بطاقات الائتمان على أدارة الدخل المالي للأسرة السعودية" .رسالة ماجستير.قسم السكن وأداره المنزل.كلية التربية للاقتصاد المنزلي والتربية الفنية بجدة:1491هـ.1999م.
- 24 - لطفي ، فاتن مصطفي كمال ."الإدارة العلمية لشؤون الأسرة " .سهير فؤاد نور.الطبعة الأولى . الأمارات العربية المتحدة .دبي .دار القلم للنشر والتوزيع.1423هـ.2003م .
- المصدر :نعمون وهاب، "مرجع سابق" ،ص: 274.
- المصدر :نعمون وهاب، "النظم المعاصرة لتوزيع المنتجات المصرفية وإستراتيجية البنوك" ، مداخلة مقدمة إلى ملتقى المنظومة المصرفية الجزائرية والتحولات الاقتصادية - واقع وتحديات - جامعة حسيبة بن بوعلي، الشلف - الجزائر، يومي14/15 ديسمبر 2004، ص: 273.
- المصدر :تبول الطيب، "سياسات التجارة الالكترونية والمسائل القانونية"، مقال منشور على الانترنت على الموقع
- المصدر : عز الدين كامل أمين مصطفي، " الصيرفةالإلكترونية" ، مقال منشور على الأنترنت على الموقع
- الديوان الوطني للرقابة المالية في المملكة المتحدة (NAO)، ترجمة الساطي، طارق (1989) إطار الرقابة المالية على مردود إنفاق الأموال العامة (رقابة الأداء) ص5 ويوجد الكتاب على الموقع التالي:
- /http://www.saiuae.gov.ae
- تركستاني، أنيسة (2007). المحاسبة الإدارية، الموقع الالكتروني ، (www.anisaht.com).

- جولدبرج، مايكل وجريس، لورنا وهلمس، بريجيت، وآخرون (2002). التحليل المالي، المجموعة الاستشارية لمساعدة الفقراء CGAP ، ترجمة شبكة التمويل الأصغر في البلدان العربية - سنابل وبتمويل من مؤسسة روكديل. وتوجد نسخة من الكتاب على شبكة الانترنيت وعلى العنوان التالي: (www.cgap.org).
- حوار للكاتب أحمد الفهيد مع الدكتور صالح العمير رئيس مجلس إدارة شركة اوركس السعودية،
- أبو نصار، محمد حسين (2005). المحاسبة المالية المتقدمة، عمان، دائرة المكتبة الوطنية، ط1.
- الجمعية السعودية للمحاسبة (2005). المعلومات المحاسبية ودورها في أسواق الأسهم، جامعة الملك سعود، المملكة العربية السعودية.
- الجمعية السعودية للمحاسبة (2006). تحليل القوائم المالية وعلاقتها بسعر السهم، جامعة الملك سعود، المملكة العربية السعودية.
- الحبيطي، قاسم محسن والسقا، زياد هاشم (2003). نظم المعلومات المحاسبية ، الموصل ، العراق، الناشر وحدة الحدباء للطباعة والنشر ، كلية الحدباء الجامعة.
- الحيالي، وليد (2004). الاتجاهات المعاصرة في التحليل المالي، عمان، الأردن، مؤسسة الوراق للنشر والتوزيع، ط1 .
- الحيالي، وليد (2007). مذكرات في التحليل المالي، الدنمارك، منشورات الأكاديمية العربية المفتوحة في الدنمارك.
- الحيالي، وليد والبطمة، محمد عثمان (1996). التحليل المالي، عمان، دار حنين، ط1.
- السالم، مؤيد سعيد (2005). نظرية المنظمة، عمان، دار وائل للنشر، الطبعة الثانية.
- الصباح، عبد الرحمن (1989) الرقابة الإدارية بين النظرية والتطبيق، جامعة الإسكندرية.
- الصباح، عبد الرحمن (1996). مبادئ الرقابة الإدارية المعايير والتقييم والتصحيح، عمان، دار زهران .
- الصياح، عبد الستار مصطفى و العامري، سعود جايد (2006). الإدارة المالية، عمان، دار وائل للنشر، الطبعة الثانية.

- القاضي، دلال وعبد الله، سهلية والبياتي، محمود (2003). الإحصاء للإداريين والاقتصاديين، عمان، دار الحامد للنشر والتوزيع.
- القريشي، أياد رشيد والجعفري، وسن عبد الصمد (2006). دور مراقب الحسابات ومسؤوليته في تلبية احتياجات مستخدمي القوائم المالية، المعهد العربي للمحاسبين القانونيين، جامعة بغداد.
- المؤسسة العامة للتعليم الفني والتدريب المهني (2003). مراجعة ومراقبة داخلية، المملكة العربية السعودية.
- المؤسسة العامة للتعليم الفني والتدريب المهني (2003). الموازنات وإعداد التقارير، المملكة العربية السعودية.
- المؤسسة العامة للتعليم الفني والتدريب المهني (2003). مبادئ إدارة الأعمال، المملكة العربية السعودية.
- الموسوي، سنان (1999). إدارة الموارد البشرية وتأثيرات العولمة عليها، عمان، دار الحامد للنشر والتوزيع، الطبعة الأولى.
- الهواري، سيد (1994). الإدارة الأصول والأسس العلمية، القاهرة، مكتبة عين شمس.
- توفيق، محمد شريف (2006). إعداد القوائم المالية المخططة " المتنبأ بها" ، جامعة الزقازيق، كلية التجارة.
- ربابعة، عبد الرءوف وحطاب، سامي (2006). التحليل المالي وتقييم الأسهم ودور الإفصاح في تعزيز كفاءة سوق الأوراق المالية، هيئة الأوراق المالية والسلع، الإمارات العربية المتحدة.
- عاشور، احمد صقر (1985). الإدارة العامة مدخل بيئي مقارن، الإسكندرية، دارة المعرفة الجامعية.
- عبد الله، عقيل جاسم (1999). تقييم المشروعات "إطار نظري وتطبيقي" ، عمان، دار مجدلاوي للنشر، الطبعة الثانية.
- عدنان تايه والساقي، سعدون مهدي وآخرين (2007). الإدارة المالية، عمان، دار المسيرة، ط1.
- عشماوي، سعد الدين (1980). أسس الإدارة، القاهرة، مكتبة عين شمس.

- عقل، مفلح محمد (2006). مقدمة في الإدارة المالية والتحليل المالي، عمان، مكتبة المجتمع العربي للنشر والتوزيع، ط1.
- علاقي، مدني عبد القادر (1985) دراسة تحليلية للوظائف الإدارية والقرارات الإدارية، جدة، مكتبة تهامة.
- عمر، محمد عبد الحليم (1991). تقييم الكفاءة والفعالية في البرامج الحكومية، الرياض، كلية العلوم الإدارية، جامعة الملك سعود.
- قاسم، صبحي المحمد (1996). مقدمة في بحوث العمليات، عمان، مؤسسة آلاء للطباعة والنشر، الطبعة الأولى.
- مرعي، عبد الحي و الصبان، محمد سمير (1988). أصول المحاسبة المالية، بيروت، الدار الجامعية.
- مطر، محمد عطية و الحيالي، وليد ناجي، الراوي، حكمت احمد (1996). نظرية المحاسبة واقتصاد المعلومات.عمان، دار حنين، ط1.
- منصور، علي محمد (1999). مبادئ الإدارة أسس ومفاهيم، القاهرة، مجموعة النيل.
- مهدي، محمود كمال والقريشي، أياد رشيد (2001). الإجراءات التحليلية في التدقيق، المعهد العربي للمحاسبين القانونيين، جامعة بغداد.
- د. محمد يونس خان ، د. هشام صالح غرابية ، الإدارة المالية ، جون وايلى وأولاده ، 1986م ، ص 13 – 15 .
- د. منير إبراهيم هندى ، الإدارة المالية : مدخل تحليلى معاصر ، المكتب العربى الحديث ، الإسكندرية ، 1997م ، ص 19 ، 21 .
-

- tter.darryl E. Consumer credit: Broader availability, deeper debt. Journal of Retail Banking services.Iss, 1.Vol.18 (spring: 1996).
- Mapother Bill .the real Cause of Bankruptcy Credit Union Magazine (Jun; 1995).
- Ranyrard .rob and Craig .Gill. Evaluating and Budgeting with installment credit: An Interview Study. Journal of Economic Psychology. (1995)

- http://www.arabrenewal.org/blogs/2101/CaEOIa-Yi-CaOUacIiE-iOIa-AUai-aOEaciCEa-Yi-10-AUacCa-aciaCaO-5-.html
- Gunnar, Rimmel & Christian, Nielsen (2006). Företagsekonomi, Studentia, Sweden
- Olsson, Karl O. & Olsson, Magnus (2006). Finansiering, Sweden, Göteborgs Universitet
- Frank J. Fabozzi & Pamela P. Peterson (2003). Financial management & analysis, John Wiley & Sons, Inc, Second Edition.
- Levy, H. and M. Sarnat, Capital Investment and Financial Decisions , N.J. : Prentice – Hall, 1990, P. 10.
- financial management & analysis frank j.fabozzi & Pamela Peterson / 2003/ (second edition)
- fundamentals of financial management (10 edition) Brigham &3Houston

فهرس